INTEGRATION OF CYBER SITUATIONAL AWARENESS INTO SYSTEM DESIGN AND DEVELOPMENT

GRADUATE RESEARCH PROJECT

Lee E. Chase, Major, USAF

AFIT/ISE/ENV/09-J02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ISE/ENV/09-J02

INTEGRATION OF CYBER SITUATIONAL AWARENESS INTO SYSTEM DESIGN AND DEVELOPMENT

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Systems Engineering

Lee E. Chase, BS, MA

Major, USAF

June 2009

AFIT/ISE/ENV/09-J02

INTEGRATION OF CYBER SITUATIONAL AWARENESS INTO SYSTEM DESIGN AND DEVELOPMENT

Lee E. Chase, BS, MA
Major, USAF

Approved:

_____/signed/_____ _____
John M. Colombi, PhD (Chairman) Date

_____/signed/_____ _____
Robert F. Mills, PhD (Member) Date

Abstract

Cyber Situational Awareness (SA) is the correlation of network status to operational mission impact. This capability is increasingly important for commanders and individual weapon system platforms as the DoD continues its exploitation of network-centric operations. To achieve higher maturity levels of cyber SA, the acquisition community needs to act as an enabler by making cyber issues an integral part of early system design and development. This paper identifies key cyber characteristics needing consideration and recommends improvements to acquisition policy and guidance, including the net-readiness key performance parameter (NR-KPP) and the DoD Architecture Framework (DoDAF).

Acknowledgements

I would like to thank my research advisors, Dr. John Colombi and Dr. Robert Mills, for providing much wisdom and insight in guiding me through a such a broad and complex problem. There is still much to discuss and learn regarding cyber situational awareness, and it is only with their assistance that this research project is hopefully able to shed some light upon the topic.

I also owe a huge debt of gratitude to my wife and four kids who unceasingly provided words of encouragement during the long hours and, at times, frustrations associated with this research project. Their words, smiles, and constant support were integral to this effort, and any value that results is attributable to them as much as it is to me.

Lee E. Chase

Table of Contents

Page

Page

List of Figures

List of Tables

Table Page

INTEGRATION OF CYBER SITUATIONAL AWARENESS INTO SYSTEM DESIGN AND DEVELOPMENT

I. Introduction

Background

Cyberspace, as defined by Joint Publication 1-02, is "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Joint Staff, 2009: 141). This definition emphasizes cyberspace as its own operational domain, equivalent to the other operational domains of air, land, and sea. This perspective is shown in the left side of Figure 1. In this concept, cyberspace can create similar warfighting effects to the other warfighting domains of land, sea, and air. For example, cyberspace can be used to gain entry into an adversary's networks to take out their electrical grid or to implant false information into the adversary's information systems to provide them an incorrect picture of our next military operation.

However, the understanding of cyberspace as its own domain only presents part of the picture with regards to the functions and importance of cyberspace. Another common perspective of cyberspace is that it is primarily an infrastructure to support military operations in other domains (Figure 1 right).

In this perspective, cyberspace is seen as a tool to pass information, gather intelligence, and improve communication in support of the air, land, sea, and space domains. Ultimately, through the use of cyberspace, the other domains can experience an

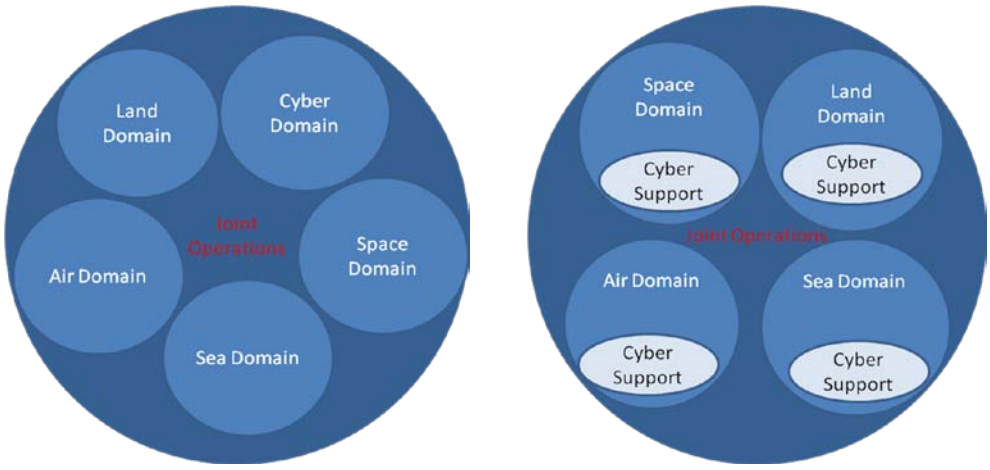

Figure 1 – Cyberspace as its own Warfighting Domain (left)
or as Supporting Infrastructure (right)

increased pace of operations and improved efficiency, facilitating friendly forces getting inside the adversaries observe, orient, decide, and act (OODA) loop. Both perspectives of cyberspace are correct and both need to be properly considered in order to develop a comprehensive approach to cyberspace operations and associated cyber situational awareness (SA).

The cyberspace perspective one takes drives the types of activities in developing cyber SA. A focus on cyberspace as its own operational domain tends to drive cyber SA activities required for attacking the adversary's networks and defending our own networks. From an offensive standpoint, cyber SA activities include understanding the layout of the adversary's networks, assessing their network vulnerabilities and cyber defense capabilities, and developing an understanding of how attacks on particular aspects of their networks will produce effects. Cyber SA activities in support of cyber defense operations are similar to cyber SA activities in support of cyber attack activities, but of course are focused upon our own networks. These activities include understanding

the adversary's intent and capabilities, understanding our own network layouts and vulnerabilities, having a real-time understanding of current intrusions in our networks (e.g. malware, network sniffers, malicious code), and knowing what effects will likely result.

For the most part, the cyber SA activities described above for cyber defense operations are the same cyber SA activities needed to support cyberspace when it is primarily seen as a supporting infrastructure to other warfighting domains. However, one key difference between the two is the perspective taken with regards to understanding the "effects" resulting from an adversary's attacks upon our networks. In practice, when discussing "effects" from a perspective of cyberspace as its own operational domain, "effects" tends to refer to the degradation or failure of a particular connection, service, or piece of hardware in the network (i.e. server, computer, etc.). The focus is on the network itself, not the military operations it is supporting. When viewing "effects" from the perspective of cyberspace as a supporting infrastructure to other warfighting domains, however, it becomes tied to military operations. Effects no longer end with the physical make-up of the network, but are now tied to likely outcomes of military operations. It is this definition of cyber SA, the correlation of network status to operational impact for which this research is concerned.

The need for establishing cyber SA has gained rising importance as the DoD has become more and more network centric in its operations. The use of cyberspace has significantly increased the amount of information flowing to the commander, providing opportunities for increased situational awareness and the ability to make more informed decisions. In addition, the use of the cyber infrastructure has allowed the DoD to

interconnect a large number of its weapon systems, turning our armed forces into a systems of systems that produces warfighting capabilities and effects never previously envisioned. Individual weapon systems themselves are becoming heavily reliant upon the network to pass information, detect targets, receive intelligence, enable remote operations, etc., for successful accomplishment of the mission. Unmanned aerial vehicles (UAVs) such as Predator and Global Hawk are remotely operated from thousands of miles away while gathering intelligence that is fed back through the network to operations centers or directly to troops on the ground to engage time-critical targets. Newer air platforms such as the F-22 and Joint Strike Fighter (JSF) are implementing leap-ahead technology, often enabled by a significant increase in their network-connectedness. Although this network-centric force results in improved capabilities that keep the United States ahead of many of its adversaries in waging war, it also results in significant operational risks.

It is a well-known fact that the cyber domain has much vulnerability and provides an avenue for an adversary to degrade our capabilities at fairly low cost. Whether it is a terrorist organization who attempts to wage unconventional warfare or a nation-state that desires to degrade our capabilities, steal our technology, or alter our understanding of the battlespace, the cyber domain provides an attractive option. As such, it is important that the operational commander have an understanding of the current status of the network upon which he or she relies. This cyber situational awareness (SA) is key to the commander for several reasons. First, the commander needs to know the reliability of intelligence being provided for situational awareness. If cyber incidents are taking place that could be causing a reduction in the accuracy of the information being received, the

commander needs to take this into account in making decisions. This large area of results examines trust in automation or trustworthiness of data. Secondly, if the commander is authorizing particular operations, he needs to know if the overall cyber infrastructure (i.e. communication lines, computer networks) is sufficiently secure during the timeframe of the operations to adequately complete the missions at an acceptable success rate. Third, the commander needs to know if individual weapon systems used during operations can successfully accomplish the mission based upon the cyber configuration and status. The commander, in order to have cyber SA at any given time, needs to answer questions such as the following:

- Can weapon systems receive accurate and timely mission intelligence for planning?
- What is the predicted reliability of command and control links to individual platforms during a mission?
- Are there any network information links or resources unavailable that tasked weapon systems are reliant upon for completing the mission?
- Do the weapon systems have workarounds for accomplishing the mission even if key infrastructure becomes unreliable before or during the mission?
- Is there suspected adversary activity in weapon system databases, information repositories, etc. that reduces our data assurance reliability?

The problem is that DoD currently cannot provide answers for these type of cyber SA questions to the commander (Grimaila and Fortson, 2007:206), leaving the commander with significant uncertainty during decision making processes.

Solving the problems mentioned above and creating quality cyber situational awareness for the commander is not a simple task, however. It is a multifaceted problem involving many subelements. Several subelements that could be included in the development of an adequate cyber SA picture include the following:

- Intelligence assessments of foreign country cyber networks, to include intentions, capabilities (both offensive and defensive), and vulnerabilities
- Tools for detecting cyber attacks
- Methodologies for assessing the impact of cyber incidents upon operational missions
- Tools to consolidate assessments and correlate mission impacts in an easy to understand format for the commander
- Methodologies for including cyber SA considerations during system design

Significant effort will be required to develop mature capabilities in each of these subelements along with integrating them to provide a robust cyber SA capability. In several of these areas, some degree of effort is already being applied. For example, intelligence assessments of foreign country cyber capabilities, to include both computer network attack and computer network defense capabilities, are being performed by US intelligence agencies. Private industry, along with the DoD, has invested significant dollars in the development of tools, such as intrusion detection devices and antivirus software, for detecting attacks. Initial research is being conducted on developing methodologies for assessing the impact of cyber incidents upon operational missions. As an example, the Cyber Incident Mission Impact Assessment (CIMIA) research program at the Air Force Institute of Technology (AFIT) and the Air Force Research Laboratory

(AFRL) has a stated goal of "developing an operational methodology that organizations can use to assist in the identification, valuation, documentation, and reporting of critical information asset dependencies in order to provide near real time cyber damage and mission impact assessment" (Grimalia and others, 2008:10).

Each of the subelements listed above will continue to require focused research and resourced efforts to mature cyber SA to the needed level. The purpose of the research in this paper is to direct some of the research and thought at ensuring cyber SA is considered during system design and development. To some degree, the DoD has already increased its focus on ensuring cyber related issues are addressed during system design and development. This can be seen in Defense Acquisition University courses on systems engineering where an emphasis is placed on network interoperability between systems. In addition, the DoD has established a net readiness key performance parameter (NR- KPP) to assist in adequately preparing weapon systems for the net-centric environment in which they are expected to operate. The NR-KPP is mandatory for all acquisition information technology (IT) and National Security System (NSS) programs used to enter, process, store, display, or transmit DoD information, regardless of classification or sensitivity. The only exception to the NR-KPP requirement is IT and NSS programs that do not communicate with external systems (Joint Staff, 2008: E-1). However, in today's environment, since it is rare for a system to not communicate with some external system, the vast majority of acquisition programs are required to comply with the NR-KPP. Although these efforts have been initiated by the DoD to address cyber related concerns during the design and development of weapon systems, it is

questionable as to whether or not concerns specifically related to SA in the cyber domain have been adequately addressed.

Before developing recommendations on how to ensure cyber SA concerns are addressed during system design and development, this paper will first examine a general definition of SA. Current DoD doctrine and operating concepts will be examined and used to apply the general definition of SA to the cyber domain. Current operational and acquisition related efforts related to cyber SA will be reviewed to determine their adequacy in meeting full cyber SA requirements. Based upon existing shortfalls, the paper will provide thoughts and recommendations regarding what the acquisition community can contribute during design and development of weapon systems to ensure a more robust cyber SA capability.

Problem Statement

In order to provide a robust process for delivering cyber SA to the commander, it is necessary to include cyber SA concerns and principles during system design and development. To ensure appropriate inclusion, two steps need to be taken. First, better definition of cyber SA requirements for acquisition is needed to ensure critical cyber SA concerns are addressed during system development. Secondly, the defined cyber SA requirements for acquisition need to be adequately incorporated into DoD acquisition policies and guidance to ensure they are being appropriately assessed during system design and development. This research will address these two steps in an effort to improve the acquisition's community's contribution towards providing a robust and trusted cyber situational awareness picture.

Research Questions

To solve the cyber SA problem, contributions from both the operational and acquisition communities are needed. To determine where and how the acquisition community can contribute, the following questions need answered:

I. What should be the derived cyber SA requirements for all acquisition?

II. How does the current NR-KPP assess cyber SA requirements?

   a. Does the current NR-KPP adequately address cyber SA requirements for NSS and IT systems?

   b. Does the J-6 certification process of the NR-KPP through the Information Support Plan (ISP) ensure proper levels of useful documentation

   c. Does Information Protection (IP) activities within the NR-KPP adequately address weapon ssystem cyber SA needs?

III. What additional policies need to be integrated into DoD acquisition documentation to ensure adequate integration of cyber SA requirements into weapon system design and development?

   a. Does new language need to be inserted into DoD and AF-level directives and/or instruction?

   b. Do changes need to be made to current NR-KPP guidance?

   c. Are alterations to DoDAF architecture products required?

Methodology

A comprehensive review of existing literature and documents pertaining to the research focus will be conducted. These findings will be augmented by interviews with appropriate functional experts. Through these efforts, an understanding of what the key derived cyber SA requirements for acquisition will be developed. A comparison between the developed cyber SA requirements for acquisition and current acquisition policy and guidance will be conducted. From this assessment, recommendations regarding changes

to current acquisition policy and guidance will be provided to ensure cyber SA is addressed during system design and development.

Limitations

The results from this research will identify the key analysis required during system acquisition development to improve a weapon system's contribution to an operational commander's cyber SA picture. As such, this study is only addressing the cyber SA subelement of developing methodologies for including cyber SA in system design and development. It is left to other research for the continued investigation of other cyber SA subelements mentioned previously (i.e. development of tools for detecting cyber attacks, development of methodologies for assessing the impact of cyber incidents upon operational missions, and development of tools to consolidate assessments and impacts in an easy to understand format for the commander). In addition, recommendations for the acquisition community will primarily be at the policy/guidance level to ensure weapon systems in design and development are adequately addressing cyber SA. Consequently, the goal of this research is not to provide a checklist of specific data, protocols, formats, etc., that meets every weapon system's cyber SA needs. Instead, the goal is to ensure a mechanism is put in place, so that during early design, the necessary cyber SA requirements will be considered by each weapon system.

II. Literature Review

Situational Awareness – Endsley Model

A well-recognized situational awareness framework is provided by Endsley (Figure 2). Specifically, Endsley defines SA as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" (Endsley, 1988). Within the framework of this definition, Endsley defines three levels of SA.

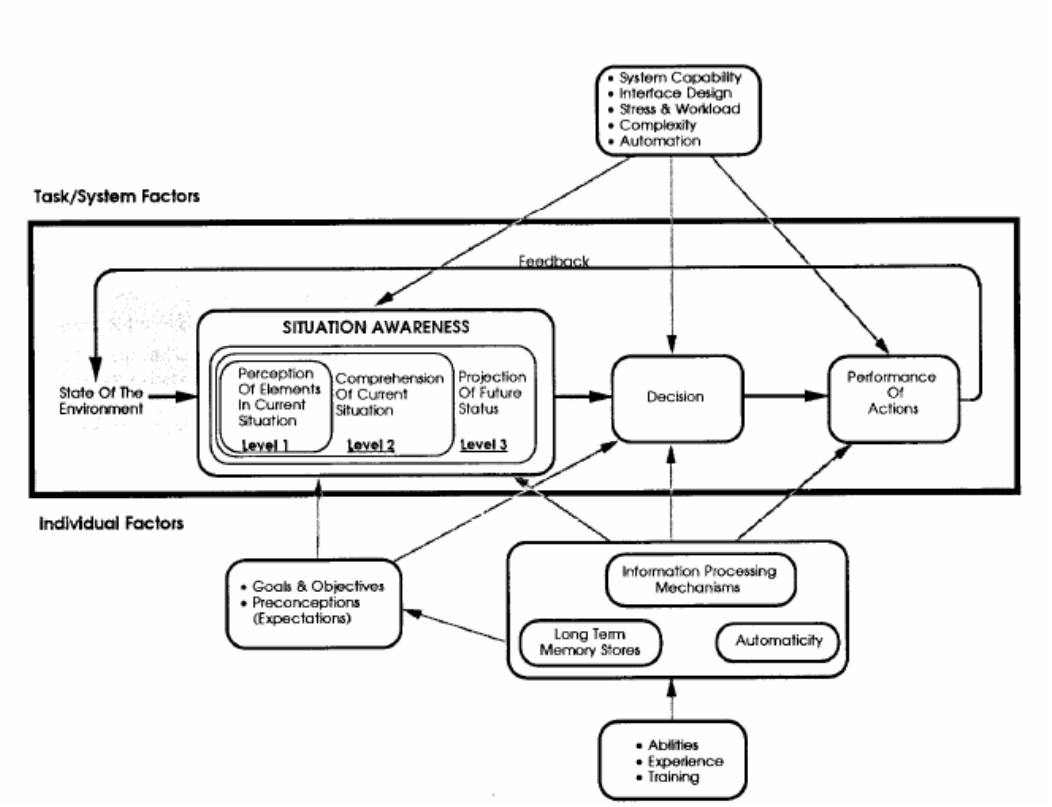

Figure 2 Model of Situational Awareness (Endsley, 1995:35)

1. Level 1 SA, perception, refers to recognizing the proper information required for the situation at hand. In other words, it is the ability to identify the correct pieces of

information, or cues, from the myriad of information that can be present at any particular time (Endsley, 2000:3).

Level 2 SA, comprehension, involves the ability to take all the important bits of information available and integrate the information in a way that allows a person to determine its relevance to their goals. A person, using the information gathered from their Level 1 SA, can "derive operationally relevant meaning and significance" (Endsley, 2000:4). In essence, Level 2 SA is a person's interpretation and application of Level 1 SA to goals that have been previously set.

Level 3 SA, projection, involves the ability to predict future scenarios or situations. The ability to achieve Level 3 Projection SA is critical for allowing decision makers to make timely and beneficial decisions for themselves or their organization (Endsley, 2000:4). It is at Level 3 where SA provides the most "bang for the buck." Achieving Level 3 projection allows a person or organization to be proactive versus reactive.

Another critical aspect of Endsley's definition is the temporal aspect of SA (Endsley, 2000:4). In many instances, including the military environment, the information available for assisting with SA is constantly changing. As a result, a person's SA needs to be constantly changing in conjunction with the new information arriving. Otherwise, a person's SA will quickly become inaccurate or irrelevant.

It is also important to note the goodness of a "decision" which follows the establishment of SA is not always directly related to the goodness of the SA. In other words, decision makers can make poor decisions even with very good SA. Or, even when good decisions are made based upon the current SA, unexpected factors outside of

the control of the decision maker may interfere, resulting in failure. On the other hand, success may result even if the decision maker has poor SA (Endsley, 2000:5). The bottomline is that improved SA should improve the odds of correct choices and the obtainment of goals.

Intertwined with the different levels of SA and its associated temporal aspects is the realization that SA at any given time is highly cognitive, and as a result, will differ between individuals. As shown previously in Figure 3, factors such as training and experience, along with cognitive abilities such as long term memory stores will result in one person being able to achieve better SA than another person given the same information.

In conclusion, several key takeaways can be derived from the general definition of SA presented above:

1. Level 3 SA is the desired end state, especially within the military realm. Level 3 SA allows a commander/decision-maker to be proactive as opposed to reactive. By achieving Level 3 SA, the military commander is able to take the initiative and get inside an adversary's Observe, Orient, Decide, and Act (OODA) loop.
2. Although Level 3 SA is the desired end state, it doesn't reduce the importance of Level 1 and Level 2 SA. Level 1 and 2 SA are prerequisites for achieving Level 3 SA, and if not done appropriately, can create significant problems with Level 3 SA. At the best, significant inefficiencies (i.e. increased time, increased resources) will result in achieving Level 3 SA. At the worst, the

odds of harmful decisions being made can be significantly increased if Level 1 and 2 SA are incorrect.

3. Time is of the essence. This is especially applicable to the military realm due to the fluid nature of military operations and the constantly changing nature of the battlefield. As a result, a worthwhile level of SA often needs to change based upon the environment in which a decision maker is operating.

Cyber Situational Awareness - DoD Doctrinal Perspective

From a DoD perspective, SA is often interchangeably used with the term battlespace awareness. The Joint Functional Concept for Battlespace Awareness (BA) defines battlespace awareness as:

> The situational knowledge whereby the Joint Force Commander plans operations and exercises command and control. It is the result of processing and presentation of information comprehending the operational environment – the status and dispositions of Friendly, Adversary, and non-aligned actors; and the impacts of physical, cultural, social, political, and economic factors on military operations....BA provides commanders and force elements with the ability to make better decisions faster by enabling a more thorough understanding of the environment in which they operate, relevant friendly force data, the adversaries they face, and non-aligned actors that could aid in or detract from friendly battlespace success (JROC, 2003:10).

Lumped into this definition are many of the same elements found in the three different levels of SA described by Endsley. The processing and presentation of information comprehending the operational environment integrates both Level 1 and Level 2 SA, while Level 3 SA is seen in the desire to "make better decisions faster." The BA functional concept also briefly highlights the cyber domain, citing the need to "include sources and methods that allow for the detection of hostile actions as well as identifying

adversary capabilities and forecasting adversary intent in the cyber realm" (JROC, 2003:29).

The Deterrence Joint Operating Concept, Version 2.0 (USSTRATCOM, 2006:29), defines SA as the "operational intelligence information about adversary assets, capabilities, and vulnerabilities required to conduct credible and effective deterrence operations." It also goes on to state,

> successful deterrence also requires much improved understanding of our own capabilities, limitations, and current situation (blue force tracking and force status, to include our allies and interagency partners). Such understanding is achieved through exploiting shared information, awareness, and understanding of the situation across a networked infrastructure by means of a collaborative information environment. Highly networked forces will increase the commander's flexibility to choose from widely varying types of capabilities to achieve the desired deterrence effect (USSTRATCOM, 2006:31).

From this definition, we can observe that there is both an adversary and friendly aspect to SA. In order to conduct successful operations, one has to have SA not just on the status of the adversary, but also upon the status of friendly forces in order for the commander "to choose from widely varying types of capabilities."

Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (IPB), also provides some good insights into DoD's perspective of SA. In general, Joint IPB is designed to:

> enable joint force commanders (JFCs) and their staffs to visualize the full spectrum of adversary capabilities and potential courses of action (COAs) across all dimensions of the battlespace…by identifying, assessing, and estimating the adversary's centers of gravity, critical vulnerabilities, capabilities, limitations, intentions, most likely COA, and COA most dangerous to friendly forces and mission accomplishment (Joint Staff, 2000:vii-viii).

Here, the description of SA tends to focus more on the status of the adversary. However, it is interesting to note that when this same document discusses cyberspace, the focus is more towards having an awareness of the friendly forces status, not the adversary:

> The effects of the cyberspace environment should be evaluated by identifying and prioritizing those information systems and networks deemed most critical to the planning and conduct of military operations. Depending upon the criticality of the system, the effects of a data loss or even a short down time can result in a lingering ripple effect on military operations that may last days, weeks, or months. The relative vulnerability of each critical system should also be assessed: first, by evaluating the strengths and weaknesses of each of its cyberspace components, and second by identifying any backup systems, "work arounds," or redundant links (Joint Staff, 2000:II-37).

In other words situational awareness in cyberspace includes not only an assessment of the adversary's cyber networks and cyber intentions, but also an assessment of the status of friendly cyber networks and the resulting impact upon operations.

Cyber Situational Awareness - Other Perspectives

Grimalia and Fortson highlight the centrality of the information flowing over the network when discussing cyber situational awareness. They discuss the concept of "mission binding", which is a "measurement of how closely the information asset is bound to the organization's mission through its supporting information process" (2007:208). In other words, to have proper cyber situational awareness, it is not just a matter of knowing whether or not a link in a friendly or adversary's cyber network is operational, but also having an understanding of what information is flowing over the link and how it supports the operational mission of friendly or adversary forces. Along these lines, Grimalia and Fortson (2007:211) identify three key ideas essential for cyber situational awareness:

1. A commander must know all of the critical information assets that it uses in prosecuting its missions. To accomplish this, there must be formal, documented recognition of information dependencies
2. The commander must have real time SA of all of the information assets that it "owns" that may be critical to executing its mission
3. When an information incident occurs it must be communicated to all downstream consumers of the information that may depend upon it in support of their mission capability

The key is not to limit cyber situational awareness only to the physical hardware, software, communication lines, etc., that make up the network, but also to include the information that is flowing through the physical aspects of the network. Although both are important, the informational aspect of cyber situational awareness is key, because without the need to pass information, there is no need for the physical network.

Cyber SA Summary

Based upon the review of the literature and DoD documents above, a list of information elements that fall within the purview of cyber SA can be generated:

- Assessment of adversary cyber intentions
- Assessment of adversary cyber capabilities
- Understanding of friendly cyber capabilities
- Assessment of both adversary and friendly vulnerabilities
- Understanding of both adversary and friendly network layouts and status
- Understanding of information flowing over networks to include its purpose and criticality

- Understanding of effects/operational mission impact to both adversaries and friendlies resulting from network degradations
- Real-time understanding of current intrusions in friendly networks (e.g. malware, network sniffers, malicious code)

Cyber SA Applied to Endsley

Endsley has applied her SA model to pilots and the aircraft environment and has defined differing levels of SA for pilots. By applying the model in a similar manner to the operational commander and weapon systems involved in operational missions, differing levels of cyber SA can also be defined. In the aircraft environment, Endsley defines Level 1 SA as the pilot's perception of the aircraft and its systems. Data elements that make up Level 1 SA include "airspeed, position, altitude, direction of flight, weather, emergency information, air traffic control clearances, etc" (Endsley and others, 1998:1). In a similar manner, Level 1 cyber SA is the perception of link and node status within a network. Data elements that would make up Level 1 cyber SA include items like bandwidth usage, virus protection update status, memory utilization, encryption mode, number of open sockets, etc.

In an aircraft environment, Level 2 SA involves putting together the various Level 1 aircraft data elements and "determining the impact of one system's status on another, or deviations in aircraft state from expected or allowable values." (Endsley and others, 1998:2) Examples of Level 2 SA in the aircraft environment include "deviation between current altitude and desired altitude, margin to stall, available thrust, current separation from other aircraft, impact of aircraft malfunction on aircraft performance, impact of weather on takeoff/landing, etc" (Endsley and others, 1998:11-12). Likewise, Level 2

cyber SA elements include the determination of deviations in the network along with impact assessments of the network's cyber status upon other operational systems. Examples of Level 2 cyber SA could include deviation between current bandwidth usage and normal bandwidth usage across a link, deviation between current memory utilization and expected utilization within a weapon system computer, or the impact of a failed or degraded network link on the ability of a logistics database node to process information, or an on aircraft's ability to receive and process targeting data.

For Level 3 projection SA in an aircraft environment, Endsley provides the example of "not only comprehending that a weather cell—given its position, movement and intensity—is likely to create a hazardous situation, but also determining what airspace will be available for route diversions, and ascertaining what other potential conflicts may develop" (Endsley and others, 1998:2). Other examples include "projected trajectory, probability of staying reliably on route, projected periods of congestion, and predicted time aircraft can remain in present/anticipated conditions" (Endsley and others, 1998:13). Equivalent Level 3 cyber SA characteristics could include "projected duration of bandwidth congestion, projected reliability of information within a database, and impact predictions of projected network status upon operational systems. Table 1 show a comparison of the differing levels of SA in an aircraft environment to SA in a cyber environment.

Current Cyber SA Efforts

Based upon the delineation of the three different levels of cyber SA in Table 1, current cyber SA efforts can be examined to see where they fit within the cyber SA framework.

Table 1. Cyber SA Levels

Situational Awareness Level	Aircraft Environment (example)	Cyber Environment
Level 1	• Airspeed • Position • Altitude • Direction of Flight • Weather • Emergency Information • Air Traffic Control Clearances	• Bandwidth Usage • Virus Protection Update Status • Memory Usage • Encryption Mode • Number of Open Sockets
Level 2	• Deviation between current altitude and desired altitude • Margin to stall • Available Thrust • Current separation from other aircraft • Impact of weather on takeoff/landing • Impact of aircraft malfunction on aircraft performance	• Deviation between current bandwidth usage and normal bandwidth usage across link • Deviation between current memory utilization and expected memory utilization with in weapon system computer • Impact of failed/degraded network link on other system's performance (i.e. logistics database/ aircraft targeting)
Level 3	• Projected trajectory • Probability of staying reliably on route • Projected periods of congestion • Predicted time aircraft can remain in present/anticipated conditions	• Projected duration of bandwidth congestion • Projected reliability of data within a database • Predictions of impact on other operational systems due to network failures/degradations • Estimated traffic patterns

JTF-GNO Situational Awareness Reports

Operationally, the primary cyber SA efforts are being led by the Joint Task Force – Global Network Operations (JTF-GNO) whose mission is to "direct the operation and defense of the Global Information Grid (GIG) across strategic, operational, and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence, and business operation." (JTF-GNO Mission, 2009). As part of this mission, some of their primary responsibilities are as follows:

1) Identify and resolve computer security anomalies that affect the GIG's ability to support the warfighter
2) Identify significant threats to the GIG and develop, disseminate, and implement countermeasures to threats in a timely manner.
3) Assess incidents reported by Combatant Commander's, Service's, and Agency's Computer Network Defense individually and cumulatively for their impact on the warfighter's ability to carry out current and future missions (JTF-GNO Mission, 2009).

From the responsibilities defined above, many of the key elements of cyber situational awareness are included. Most importantly, JTF-GNO's mission includes not just identifying threats generically, but also analyzing them for their cumulative impact on a warfighter's ability to carry out current and future missions. This falls in the realm of Level 2 and Level 3 cyber SA. However, in practice, the level of cyber SA attained by JTF-GNO does not appear to reach Level 2/3. When the cyber situational awareness reports and products produced by JTF-GNO are surveyed, they lack substantive analysis of mission impact. Primarily, the reports are warnings regarding new worms or viruses

recently released, or new vulnerabilities discovered in software running on DoD networks. A few representative examples of the titles of 2009 SA reports from a review of the JTF-GNO website include "SA Report Neeris Worm", "Exploitation of Unpatched Powerpoint Vulnerability", and "Microsoft Internet Explorer 7 Remote Code Execution Vulnerability" (Situational Awareness Reports, 2009). These reports describe the vulnerabilities and provide recommendations for countermeasures, but they do not provide any assessment of current impact to the DoD mission. There is no assessment regarding the seriousness of the threat, what parts of the GIG have been affected, or how the affected parts of the GIG are impacting operational missions. In essence, the SA reports are more of a tool for assisting the GIG with "good hygiene" and implementation of its layered defenses than a real understanding of cyber situational awareness. At the best, these reports are providing some of the data elements required for Level 1 cyber SA.

Information Assurance Practices

As the DoD has moved towards a more net-centric and interoperable force, with increased risks of intrusion, interruption, and compromise, information assurance has continued to receive additional emphasis. Consequently, information assurance planning is now a subset of the NR-KPP and is mandatory requirement that must be addressed by all weapon systems. The level of information assurance required for a weapon system is based upon the assigned Mission Assurance Category (MAC). Systems can be assigned to MAC Levels I, II, or III, with Level I being the most critical in support of deployed and contingency forces. DoD Directive 8500-01E, Information Assurance, states that "DoD information systems shall be monitored based upon the assigned MAC and assessed risk in order to detect, isolate, and react to intrusions, disruptions, or other

incidents that threaten the IA or DoD operations or IT resources" (ASD[NII]/DoD CIO, 2007:7). So, at a broad level, the importance a particular system has toward the operational mission is defined through the information assurance process of assigning a MAC.

By definition, information assurance includes those activities that "protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" (ASD[NII]/DoD CIO, 2007:17). These play an important part in cyber SA. For example, the level of confidentiality a commander has in the information being passed over a particular network forms part of a commander's cyber SA. Also, a commander would want to have some insight into the current or expected availability of key information resources and the networks over which the information is passed. Although important, the level of confidentiality and level of availability of a particular weapon system node or link (i.e. platform sensor, logistics database) is at most Level 1 cyber SA data. This is primarily a result of the time factor discussed by Endsley. Information assurance processes drive the design of a system towards a static level of availability and confidentiality defined by user requirements. As a result, the commander is left to assume the levels of availability and confidentiality advertised by system requirements. Since information assurance processes do not force weapon systems to develop the capability to report information assurance levels in real-time, (i.e. the real-time effectiveness of its information assurance implementation) the commander is left with uncertainty as to the real levels of information availability and confidentiality. The commander doesn't just want to know what levels of availability and integrity have been designed into the system, but also

wants to know whether or not the desired levels are actually being achieved as information is being sent to and from the system. In the end, although information assurance processes are necessary and required for weapon systems, they are not adequate for providing a full solution to the cyber SA problem.

Network Status

Red-Yellow-Green charts are a popular tool within the DoD and are used for a variety of purposes to include defining program status and risk levels within acquisition. They are also popular in situational awareness displays for providing the operator, network operations, or commander a quick perspective on various items such as a unit's mission readiness or the operational status of a satellite. In addition, they are also used in displays for network status, reflecting items such as the current speed or congestion of various pieces of the network, or the operational status of particular nodes within the network. In some measure, these red-yellow-green status displays can provide required information needed for cyber SA, but once again, in and of themselves, do not provide the full picture required by the commander. Referring back to the description of cyber SA levels, the type of information on network status provided by such displays is typically at Level 1. Often, the display is just a visual reference to a single measurement of a network parameter. For example, for bandwidth data rates, the display may show green if above a designated speed, yellow if it is within a certain percentage of a level considered slow and red if it actually reaches the designated slow speed. As a result, the display may provide some usefulness in the establishment of Level 1 cyber SA, but little assistance in achieving the Level 2 cyber SA goal of understanding the impact of network status upon other operational systems and the resulting missions. In other words, an

operator may see that part of the network is functioning very slowly via a "red" indication on the screen, but he doesn't have anything to tell him whether or not this poorly functioning piece of the network is key to the current mission. As a result, the operator has no idea whether to devote his efforts toward resolving this particular "red" signal, resolving other "red" or "yellow" signals, or ensuring current "green" signals remain "green."

Net Readiness Key Performance Parameter (NR-KPP)

Much of the focus regarding net-centric operations within the DoD is the establishment of sufficient interoperability between systems to enable communication and the passing of data required for the mission. The NR-KPP is used as the forcing function within the acquisition community to drive this interoperability and the resulting net centricity of the DoD. This KPP is a valuable tool that is, and well continue to be, much needed in ensuring acquisition programs are putting necessary and in-depth thought into the development of interfaces and data structures. However, in the implementation of the NR-KPP and the system's resulting interfaces and data structures, the forest is often lost among the trees. In the focus to ensure correct interface profiles, standards, and data structures, the original purpose and importance of the information to the mission is often lost, and as a result not documented. In the end, the NR-KPP documentation reveals where information is being sent, through what interface profiles it is being sent, and in what formats it is being sent, while failing to identify at times which pieces of information are actually important and how that information will affect the larger operational mission if compromised or lost

One of the elements of the NR-KPP is compliance with Key Interface Profiles (KIPs). KIPs identify the most important interfaces of a system to the Global Information Grid (GIG) and provide a descriptive document specifying the technical parameters, applicable standards, and specific implementation of those standards. The goal of KIPs is to converge programs on a common set of DoD approved information technology standards to access GIG enterprise-wide services (DAU, 2009). At first look, the KIP, by the fact it is named a "key" interface profile would seem to provide some insight into which information is most important, simply by understanding what information is flowing over the KIPs versus other non-key interface profiles that may have been implemented in the system. However, when examining DoD designated KIPs maintained in the DoD Information Technology Standards Registry (DISR), it is apparent that KIPs are only common standards that provide little guidance with regards to the importance of the information flowing over them and their contribution to the operational mission. Specifying that your system uses a particular KIP such as UHF SATCOM or Global Broadcast System (GBS), for example, tells the reader that their interface is compliant with the KIP standard, but doesn't say anything with regards to the specific information flowing over the profile or the information's importance to the operational mission. So, knowing what KIPs a program has implemented provides little input towards cyber situational awareness. Instead, it only tells you that the system should connect easily to the GIG.

Although the KIP portion of the NR-KPP doesn't provide assistance with regards to cyber situational awareness, its combination with another element of the NR-KPP, integrated architectures, could provide more value. The integrated architectures, which

are described using the DoD architecture framework (DoDAF) capture operational context, a description of system nodes, communications, system functions, a mapping of operational activities to system functions, and system data exchanges. Based upon the purpose of integrated architectures, they have the potential for adding much more value towards assisting in the establishment of cyber SA for the commander.

In one sense, architecture adds value towards cyber SA by providing a description of communication links between the system under consideration and other systems, along with a description of the information being passed. However, no specifics are provided with regards to which information, and resulting nodes and links, are most critical to either the system's mission or the overall operational mission that the system is supporting. To clarify the problem, we will take a look one of the required NR KPP architecture views for milestone B, the OV-2 Operational Node Connectivity Description (Figure 3). As can be seen from the figure, activities taking place within each node are described along with information types passing between the nodes, but there is no indication of which information types are most important and to what specific activities they relate.

The current insufficiency of the NR-KPP to assist in providing adequate cyber SA to the commander is also highlighted by the Interoperability and Supportability Assessor's Checklist the J-6 uses when certifying the NR-KPP in acquisition documents and information support plans. As with the architecture products themselves, there are numerous questions related to ensuring the NR-KPP appropriately identifies interfaces, data formats, and information exchanges between nodes, but only one question regarding the relation of specific nodes and information exchange lines to operational mission

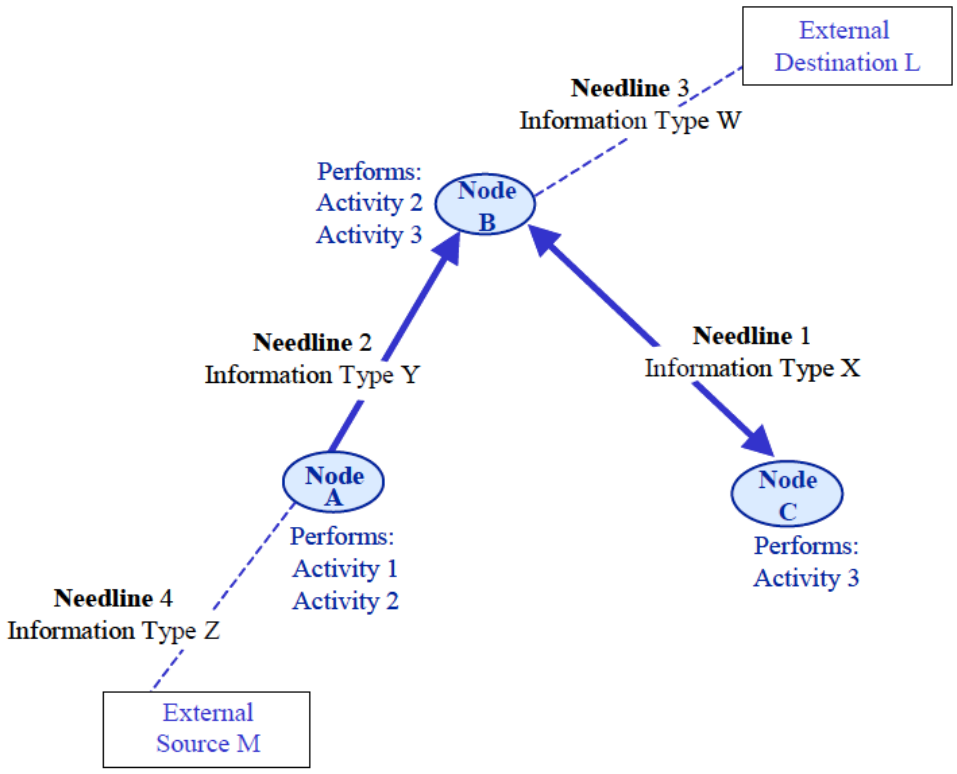

Figure 3 - OV-2 Operational Node Connectivity Description (DoDa, 2007:4-12)

impact. The one question that has applicability states, "How will the system operate in a degraded environment (limited bandwidth, changes in the information condition [INFOCON] Level)? For example, what is lost, what is the alternative method and impact on operations?" (See Appendix A for full checklist) It is interesting to note that this question does directly address the need to assess the impact of information loss resulting from conditions in the network, such as limited bandwidth, upon the operational mission. The problem, as previously shown with the OV-2 architecture example, is that the NR-KPP does not provide the tools necessary for an acquisition program to actually answer this important question.

In summary, current SA efforts are primarily providing only pieces of Level 1 cyber SA perception. As for Level 2 cyber SA comprehension (i.e. the tying of cyber status to actual operational mission impact), and Level 3 cyber SA projection there is very little existing today that can provide an operational commander with the full cyber battlespace picture information needed to make completely informed decisions.

III. Analysis and Discussion

Achieving Level 1 Cyber SA – Weapon System Cyber Status

The establishment of Level 1 cyber SA is a prerequisite for the establishment of Level 2 and Level 3 cyber SA. As discussed in Chapter II, Level 1 cyber SA is the perception of link and node status within a network. This Level 1 cyber SA for a weapon system could be designated as its "cyber status." Cyber status includes both the operating status of processors and software of the weapon system's computers along with the status of network links that are responsible for sending and receiving data to and from other weapon systems. This is true whether it is a battle management system such as Theater Battle Management Core System (TBMCS) that is primarily made up of computer hardware and processing software, or an air platform such as Global Hawk which may have several on-board sensors and processors connected to an airborne network, a Line of Sight (LOS) link for local takeoff/landing control, and Beyond Line of Sight (BLOS) communications for reachback piloting and mission analysis.

In order to establish this cyber status, the correct cyber SA data elements need to be produced, gathered, and disseminated by the weapon system to facilitate the necessary analysis required. It is the responsibility of the acquisition program during system design and development to ensure the proper tools and software are integrated to handle these cyber SA tasks. Currently, however, the ability for acquisition programs to accomplish this goal is limited due to a lack of defined cyber SA requirements from the operational community. The need for additional definition of cyber SA requirements from the operational community is needed in two areas. First, there is currently a lack of maturity regarding the specific data elements of information required to establish cyber status. Secondly, there is currently no leading community enterprise nor architecture in existence

to assist acquisition programs in understanding where the cyber SA data needs to be sent and how the data needs to be disseminated (e.g. protocols, formats).

Regarding the definition of specific data elements required for establishing a weapon system's cyber status, there is little consensus as to what such a data element set should consist. Some examples of cyber SA data elements were listed previously in Table 1, but they are not necessarily the correct data elements and are by no means comprehensive. There has been much discussion in the literature regarding which data elements or measurements are needed for establishing "network awareness." Some of these measurements include protocol state versus time, network traffic volume versus time, aggregate state of a host versus time (Hughes and Somayaji, 2005:116-117), variation in bit rate between source and destination, average time taken for bits to arrive at destination, and percent of sent bits that do not arrive at destination (Clement, 2007:17). Part of the discussion also involves awareness of the information flowing over the network, such as the current level of precision or correctness of the data (Arnborg and others, 2000:29). These information awareness measures relate to real-time measurement of confidentiality and integrity levels considered under information protection practices. As stated by Clement, "When it comes to the broad field of monitoring network performance, there is no lack of metrics to assess and tools with which to capture those metrics" (Clement, 2007:10). Due to this glut of metrics, it makes it very difficult for acquisition programs to design into their systems the right tools and software code to develop a proper understanding of the system's cyber status.

The problem is only compounded by the fact that there exists no cyber SA enterprise architecture for the DoD. The DoD Architecture Registry System (DARS),

which is the authoritative source and registry for all DoD related architecture data, has no architectural information with regards to cyber SA. If the goal is to provide a commander with the ability to understand the impact of current cyber status upon the operational mission, weapon system cyber status will have to be disseminated, combined, and correlated to make an impact assessment. Unfortunately, an architecture defining how cyber SA information will be collected, disseminated, and correlated has not been defined by the operational and cyber communities. Without this architecture, acquisition programs will have an impossible task of implementing the correct interfaces, protocols, communication links, data standards, etc. required to get the right cyber SA information to the right location in the proper format.

Pieces that would make up a cyber SA architecture can be derived from various doctrinal documents and Concepts of Operations, such as STRATCOM's Joint Concept for Operations for Global Information Grid (GIG) NetOps. Within this document, responsibility for cyber SA activities at the theater level is assigned to the Theater NetOps Control Center (TNCC) (Figure 4). The document states that the primary mission of the TNCC is "to lead, prioritize, and direct theater GIG assets and resources to ensure they are optimized to support the geographic combatant command's (GCC) assigned missions and operations, and to advise the COCOM of the GIG's ability to support current and future operations." Among its many listed responsibilities are the following two:

1. Coordinating the definition and development of the content and scope of the GIG SA information/view for the theater.

2. Direct reporting of NetOps events, conducting analysis of the impact of such events on the operational mission, developing alternate course of action (COA), and advising the Commander and other senior decision makers on the status of GIG degradations, outages, GIG network defense events, and areas requiring improvements.

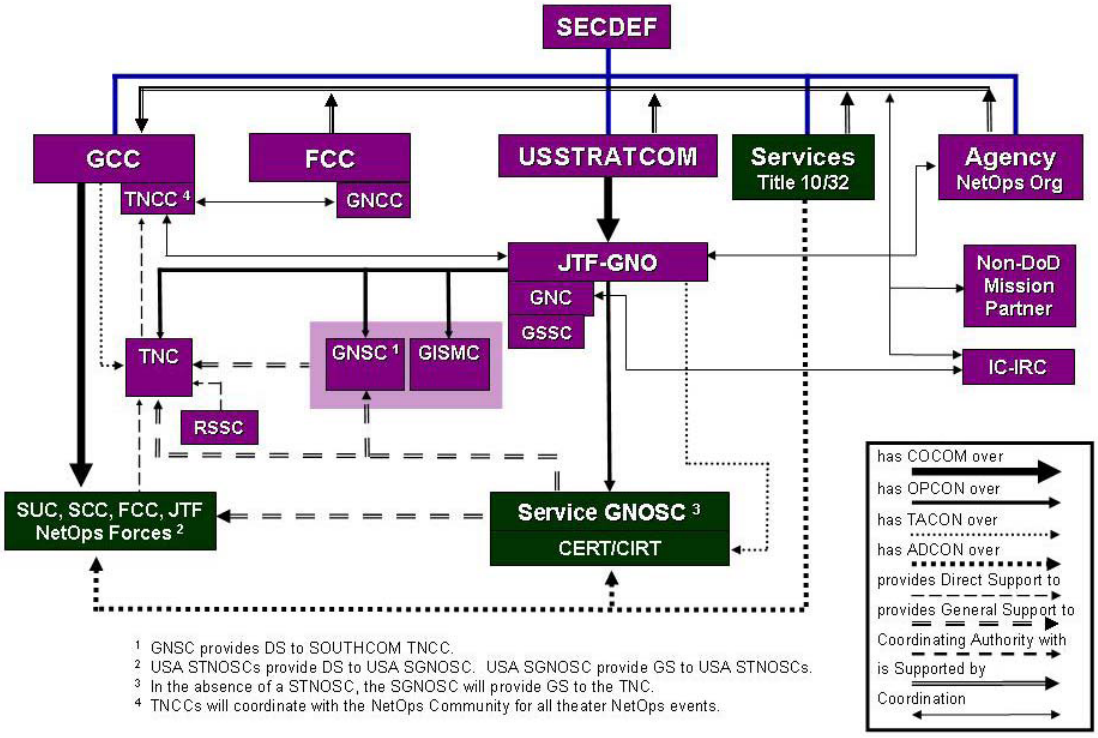

Figure 4 – Theater NetOps C2 (STRATCOM, 2006:15)

In summary, according to STRATCOM's Joint Concept of Ops for GIG NetOps, the TNCC is the combatant CC's primary resource for cyber SA, to include impact upon the operational mission. It is unclear from the document, however, exactly where the TNCC would reside in theater, who would be in charge of it, and what its layout would

look like. As a result, the current documentation does not provide the detailed information required for a mature cyber SA architecture.

STRATCOM, as the appointed lead for directing the operations and defense of the GIG, needs to work with combatant commanders and the services to develop the cyber SA architecture. This architecture should include the definitions of weapon system cyber status data elements and their formats, protocols and preferred interfaces for disseminating the cyber SA data, along with designated locations where cyber correlation will occur. This is not a simple problem and will require a significant level of effort, but it is necessary to create benefit from and synergy with acquisition programs who work to include cyber SA within their weapon system designs.

As the acquisition community works with operators and cyber experts in the development of a cyber SA enterprise architecture, one important consideration is limiting any extraneous information not related or needed for cyber SA status (Endsley, 2001:10). Limiting extraneous and unneeded cyber SA information is critical for two vital reasons. First, bandwidth is limited, especially over wireless and airborne networks. As a result, only the absolutely necessary information should be sent. Secondly, systems or personnel responsible for receiving and correlating cyber status may not have the time to sift through massive amounts of low-level Level 1 data to turn into Level 2 cyber SA or Level 3 predictions.. As the amount of unneeded information an analyst has to sift through increases, the longer it takes to do an assessment, and the more likely errors or incorrect judgments will be made.

Cyber SA Architectural Analogy – Simple Network Management Protocol

To provide some insight regarding a cyber SA enterprise architecture and the resulting derived requirements for acquisition programs, the Simple Network Management Protocol (SNMP) will be examined as an analogy. SNMP is used to monitor network-attached devices for conditions that warrant administrative attention (Case and others, 1990; DPS Telecom, undated). As shown in Figure 5, SNMP requires a software component called an "agent" which runs on each managed node or network element (i.e. router, computer, etc.) and reports information via SNMP to a network management station, or system controller. Although the diagram shows the network management station connected to only one network node/element, it can be expanded to include a large number of nodes.

The system controller, through standard commands, can retrieve specific information about the status of each managed node. For example, in a local area network, the system controller may want information on the amount of free memory or number of running processes in certain nodes. The system controller can make specific requests for information at any point in time, or through certain commands, can direct the nodes to report the desired information at specified intervals. SNMP also allows the system controller to modify and control configurations of the managed systems (Case and other, 1990; DPS Telecom, undated). For example, in a network based audio system, SNMP can allow the system controller to mute microphones (i.e. managed systems) on the network (Bruey, 2005:2).

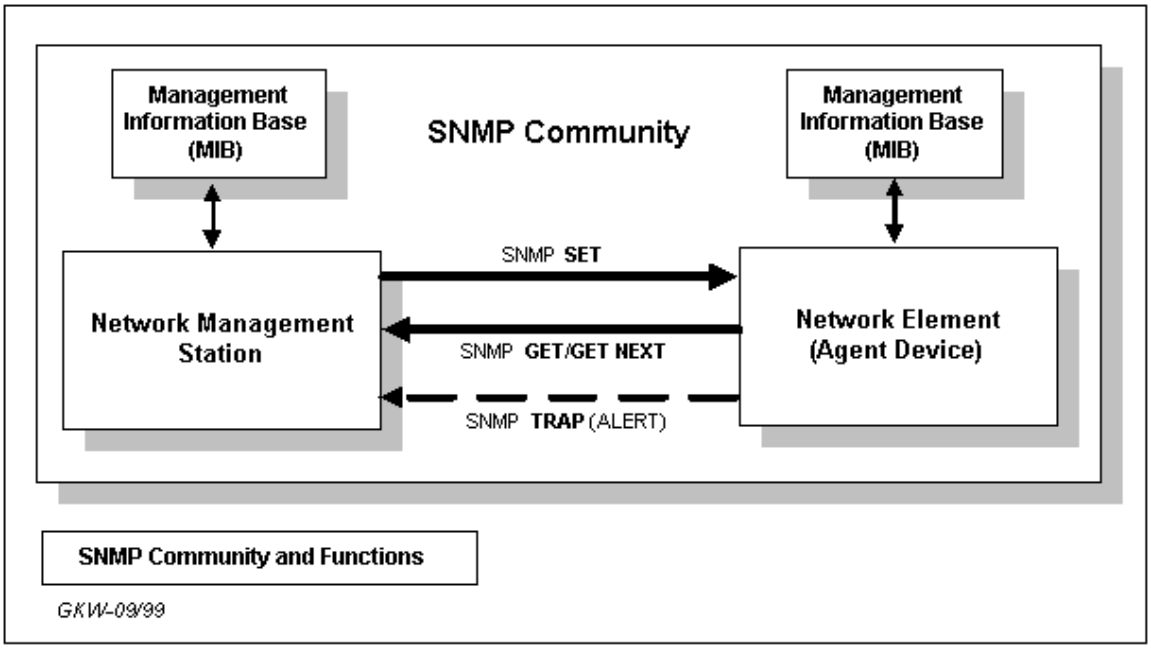

Figure 5 – SNMP Protocol (Williams Technology Consulting Services, undated)

One benefit of SNMP is that the information elements a network manager desires to control are not defined by SNMP itself. Instead, the specific information elements can be defined by the user in management information bases (MIBs). The MIB lies on both the system controller and on each managed node. Each element or piece of information listed in the MIB is assigned an object identifier (OID). When the system controller desires to know the status of a managed node, it sends an SNMP message to the node listing the specific OIDs desired. The software agent on the node looks up the OID in its MIB, finds the requested information, and sends the information back to the system controller.

In a way similar to the management of system node status within a local area network via the use of SNMP, a similar approach could be used for the management of weapon system cyber status (Figure 6 and Figure 7). The cyber correlation center would

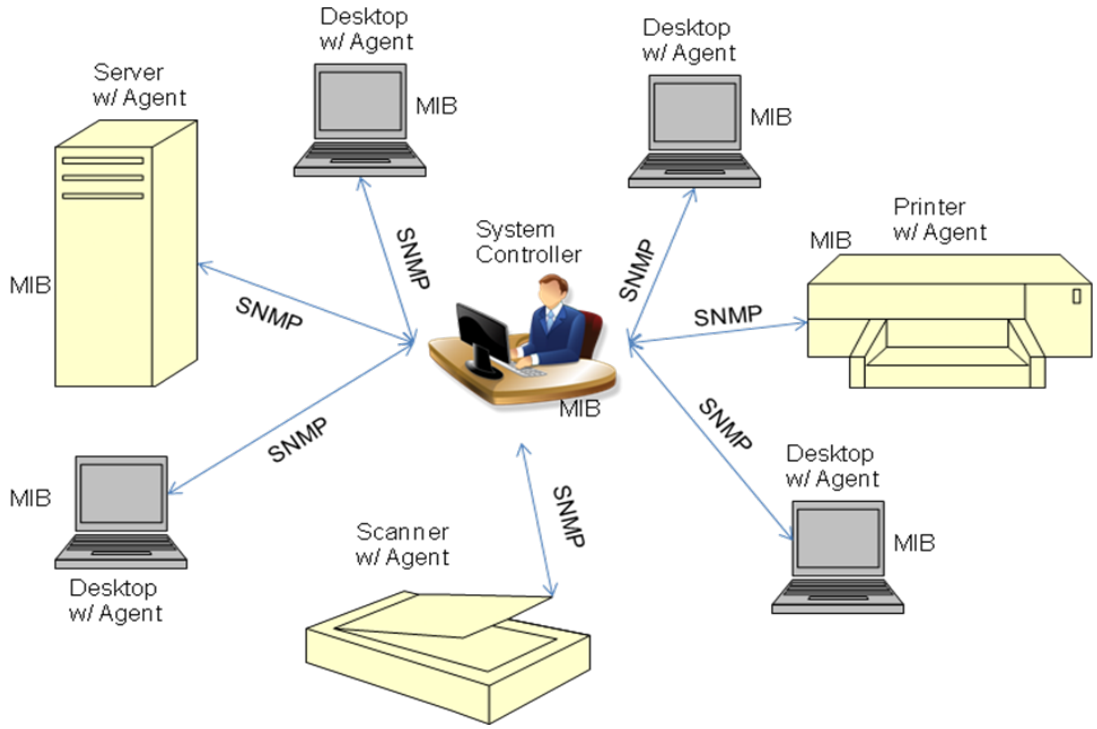

Figure 6 – SNMP Architecture

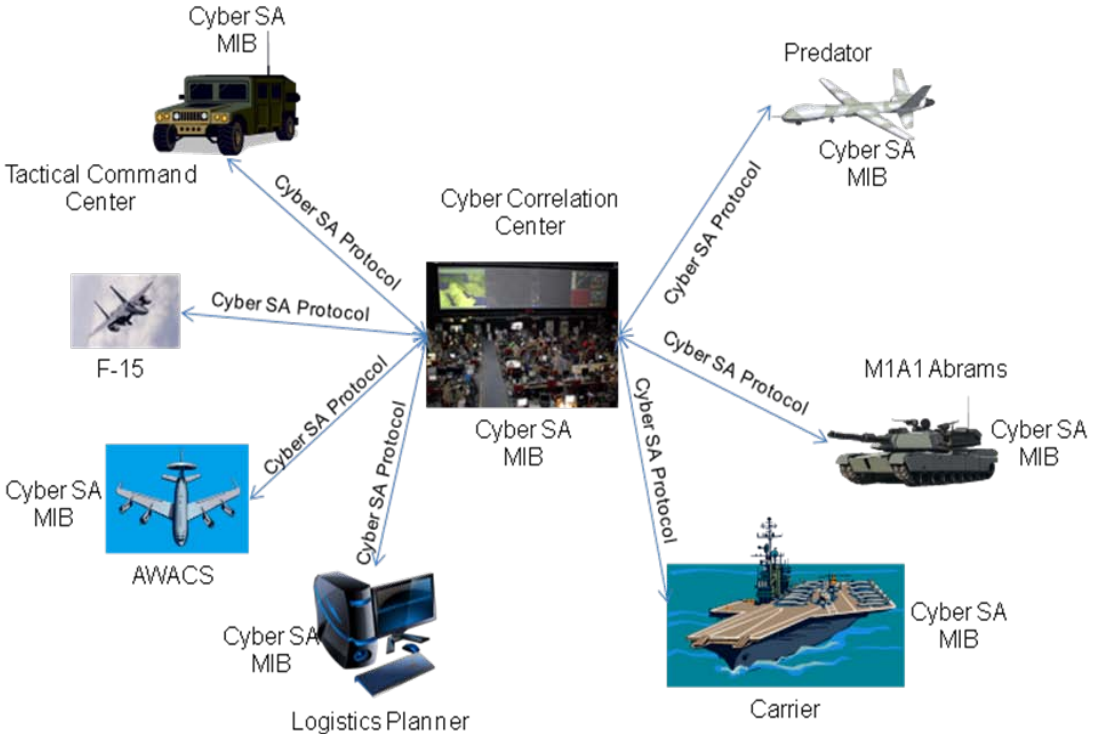

Figure 7 – Cyber SA Architecture

perform the function of the system controller in the SNMP architecture and communicate with various weapon system platforms via a cyber SA protocol. Eventually, the cyber correlation center function may be distributed. A cyber SA MIB which would contain the appropriate cyber SA elements would reside on each of the weapon system platforms along with the cyber correlation center. Ideally, if modifications to the cyber SA MIB need to be made, they can be updated in the weapon systems remotely by the cyber correlation center via the cyber SA protocol. Acquisition systems would be responsible for ensuring the cyber status MIB is loaded as an "agent" onto their weapon system and ensuring the right interfaces and communication links are implemented to connect the weapon system to the cyber SA correlation center.

Admittedly, SNMP does have several weaknesses, to include high overhead (i.e. data in the packet headers can often exceed the actual information), lack of security, and its use of the user data protocol (UDP) for the transport layer (DPS Telecom, undated). Due to these weaknesses, the scalability of SNMP to a large DoD cyber SA network is questionable, and as a result, would likely need modifications. Like all architectures, however, this one too can evolve and mature its design over time, while providing a foundation for developing solutions to the gathering and disseminating of cyber SA data. Assuming a cyber SA enterprise architecture is developed, the acquisition community then will have the derived requirements to capture the defined cyber SA data elements and disseminate them in the proper formats across the proper interfaces to the appropriate location.

Once a cyber SA enterprise architecture is defined, the NR-KPP process required during weapon system design and development should prove adequate for ensuring proper implementation and achievement of Level 1 cyber SA. The key will be for acquisition programs to ensure their cyber SA information exchanges and interfaces fit within the larger cyber SA enterprise architecture. This will ensure consistency of cyber SA data and information flows across weapon systems and the cyber SA infrastructure. Table 2 lists the essential DoDAF views for documenting cyber SA information transfer.

Table 2 – DoDAF Views Applicable to Cyber SA

Framework Product	Framework Product Name	General Description	Cyber SA Application
OV-2	Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange need lines between nodes	Show need lines from weapon system to cyber correlation site
OV-3	Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange	Document cyber SA data elements being exchanged between nodes
SV-1	Systems Interface Description	Identification of system nodes, systems and services, and their interconnections, within and between nodes	Show specific interfaces responsible for passing cyber SA data across nodes identified in OV-2
SV-2	Systems Communications Description	Systems nodes, systems and services, and their related communications laydowns	Show pathway for transfer of cyber SA data internally within specific weapon system
SV-3	Systems-Systems Matrix	Relationships among systems and services in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.	Identifies systems within weapon system node and between weapon system node and cyber correlation site node which transfer cyber SA data, and provides additional details on interfaces
SV-6	Systems Data Exchange Matrix	Provides details of system or service data elements being exchanged between system or services and the attributes of that exchange	Document cyber SA data elements being exchanged between systems identified in SV-1.

Additional Level 1 Cyber SA Activities

Although a cyber SA enterprise architecture is essential for the acquisition community to significantly contribute to cyber SA for the operational commander, there are still some proactive efforts acquisition programs can take, especially with regards to developing Level 1 cyber SA at the weapon system or platform level. First, acquisition programs should consider implementing platform based intrusion detection systems (IDSs) to record activity going to and from the weapon system across the network, and "loggers" to record activity taking place within the weapon system itself (e.g. accessing data files, changes to source code). Although the use of intrusion detection devices is fairly common today in the protection of local area networks and servers which host sensitive databases, they are much less common on weapon systems such as air platforms, ships, land vehicles, etc. As these types of platforms become more network centric and move away from proprietary tactical datalinks such as Link-16 towards more vulnerable IP-based datalinks, IDS systems becomes more important. At a minimum, these IDS systems could monitor Level 1 cyber SA data elements and provide indications and warnings to the platform operator when a potential cyber threat is detected. It is key, however, that IDSs are easily reconfigured, so that the cyber SA elements they are monitoring can be adapted to the cyber SA enterprise architecture as it is more fully developed (Salerno and others, 2005:73-74; Tadda and others, 2006:624204-2).

Similarly, acquisition programs should consider the implementation of tools such as automated malware root-kit analysis to assist in the identification of malware on system computers. Once again, although malware root-kit analysis is more commonly used on software intensive C4I systems and related databases, they should also be used

on air platforms, vehicles, etc. In many cases, having tools and standard procedures to check for malware on platform mission computers may be the only way to identify adversary activity taking place. This is especially true for those adversaries who are already in the system, either through imitation computer chips introduced during the manufacturing process or through activities not detected by an IDS. Although root kit analysis may not be able to monitor activity in real-time like an IDS, it provides another layer of capability for providing cyber SA to the platform operator.

Achieving Level 2 Cyber SA – Cyber Status Correlation to Mission Impact

As discussed in Chapter 2, some examples of Level 2 Cyber SA include deviation between current bandwidth usage and normal bandwidth usage across a link, deviation between current memory utilization and expected memory utilization within a weapon system computer, and impact of failed/degraded network links on other weapon system's performance (i.e. logistics database/aircraft targeting). The first two examples are very similar to Level 1 cyber SA information, in that the same pieces of information are being examined. The difference is that whereas in Level 1 the information is being examined in isolation, in Level 2 it is being compared to historical data that allows an analyst to make judgement calls as to whether or not something abnormal is taking place. Although a difference does exist between these two levels of information, these types of comparisons for the most part can be handled by many of the same tools (i.e. IDS's and root kit analysis tools) that gather Level 1 cyber SA type of information. Consequently, our discussion on achieving Level 2 cyber SA will not focus on these types of comparisons. Instead, the focus will be on the third example above, the taking of Level 1 cyber SA information and correlating it to impact upon other weapon systems and ultimately, the

overall operational mission. To do this, not only does the cyber status of information assets need to be understood, but the level and criticality of information dependencies between different systems is also needed.

Developing a comprehensive understanding of information dependencies to achieve Level II cyber SA is not a simple task, however. The difficulties of the task can be observed in efforts to model information dependencies within the Air Operation's Center. In this modeling effort, only one of the AOC's seven mission areas were modeled, and not surprisingly, it still resulted in a difficult and complex process that would have been compounded significantly if expanded to all seven mission areas (Shaw, 2007:78). Move beyond the AOC in an effort to expand the modeling of information dependencies between the AOC and the multiple weapon systems to which it communicates, and one can easily see the vastness of the modeling problem.

To assist in tackling the information dependency problem as a key component of achieving Level II cyber SA, acquisition programs need to accurately document their information criticalities and dependencies. Through each acquisition program doing a robust assessment, not only can Level II cyber SA at the local weapon platform be achieved, but an information dependency repository, necessary for developing Level II cyber SA for commanders at a higher level (e.g. combatant commander), can be developed. The problem that exists, however, is that current acquisition guidance does not drive the proper documentation level of information dependencies and associated criticality to support correlation of cyber status to impact upon the operational mission.

At a broad level, the assignment of a MAC to a weapon system (discussed in Chapter 2) provides a broad assessment of a system's criticality to operations based upon

the information the weapon system, generates, processes, or distributes. However, the MAC doesn't provide the detail needed with regards to the multiple pieces of information or network links that may exist on the system. For example, a system may have been assigned a MAC Level 1 due to critical information it is responsible for processing. However, when looking at the system closer, there may be multiple links to the network and other systems, of which only one is responsible for sending out the most critical information that drove the MAC Level 1 rating. In this case, even when a link or weapon system computer goes down which is not responsible for distributing critical information, the impact to operations is still assessed as critical based upon the overall system's MAC Level 1 rating. In reality, however, the impact is minor since the compromised link or weapon system computer is not carrying the critical information.

At the other end of the spectrum, the SV-6 (Figure 8) provides opportunity to assign criticality ratings (Table 3) to information being exchanged between systems, but at a level that is too detailed and isolated for a quick assessment of impact upon the operational mission. Having too much detail is primarily driven by the fact that a criticality rating is assigned to each specific information exchange, not to the network links over which the information is flowing or the weapon platform's subsystems which are generating and processing the data. Many systems may have hundreds, if not thousands of individual information exchanges. One can see the difficulty a person or system responsible for developing Level 2 cyber SA for the commander would face trying to understand the relationship of thousands of individual information exchanges, across multiple weapon systems, to operational mission impact. The challenge in assessing the loss or degradation of one or more information exchanges upon the

Interface Identifier	Data Exchange Identifier	Data Description						Producer			Consumer		Nature of Transaction		
System Interface Name and Identifier	System Data Exchange Name and Identifier	Data Element Name and Identifier	Content	Format Type	Media Type	Accuracy	Units of Measurement	Data Standard	Sending System Name and Identifier	Sending System Function Name and Identifier	Receiving System Name and Identifier	Receiving System Function Name and Identifier	Transaction Type	Triggering Event	Criticality

Interface Identifier	Data Exchange Identifier	Performance Attributes				Information Assurance							Security				
System Interface Name and Identifier	System Data Exchange Name and Identifier	Periodicity	Timeliness	Throughput	Size	Access Control	Availability	Confidentiality	Dissemination Control	Integrity	Non-Repudiation Producer	Non-Repudiation Consumer	Protection (Type Name, Duration, Date)	Classification	Classification Caveat	Releasability	Security Standard

Figure 8 – SV-6 Systems Data Exchange Matrix (DoD, 2007a:5-48)

Table 3 – DoDAF Core Architecture Data Model (CADM) Criticality Ratings for OV-3/SV-6 (DoD, 2007b:5-43)

Criticality Rating	Description
1	Mission Critical (Force C2)—Critical and high-level information (e.g., emergency action message and commander's guidance)
2	Mission Critical (Mission Operations)—Required in support to operations (e.g., joint task force contingency plans and operations plan)
3	Mission Critical (Core Functions)—Ongoing information exchanges (e.g., configuration and guidance information and restricted frequency list)
4	Mission critical [not otherwise specified]
5	Mission support—Logistics, transportation, medical (e.g., gallons of petroleum-oil-lubrication scheduled for delivery)
6	Administrative—Personnel, pay, training, etc. (e.g., change in allotment)

operational mission in a quick and accurate manner is immense. Clearly, this challenge should be an area of continued research.

In addition, the criticality ratings defined in by DoDAF's Core Architecture Data Model (CADM) may not be sufficient for providing a proper assessment of a subsystem or link's impact upon the operational mission. For example, all mission support information exchanges are given a criticality rating of 5. However the availability of logistics or transportation information may be the deciding factor for a commander in making a decision regarding the assignment of a mission. In this case, the criticality of the logistics information exchange should be much higher than 5. Increased flexibility in the criticality ratings is needed. Also, instead of assigning criticality ratings based upon functionality (i.e. Force C2, mission operations, mission support), consideration should be given towards assigning criticality ratings based upon increased risk to the commander's mission if information is lost. For example, assigning a criticality rating of 1 may indicate the inability of a weapon system to perform its mission if the information is not available. A criticality rating of 2 may indicate a significant degradation to the weapon system's capabilities, and a resulting significant increase in the risk of mission accomplishment if the information is not available. A criticality rating of 3 may indicate a minor degradation to the weapon system that creates low risk for mission accomplishment. Irregardless of the final definitions arrived at, continued improvement and refinement is needed to ensure a proper assignment of criticalities that will enable achievement of Level 2 cyber SA.

As better criticality definitions are defined, the problem of too much information in the SV-6 can be simplified by assigning mission criticality ratings to each of the links

and subsystems identified in the SV-1. These mission criticality ratings would be roll-ups of all the criticality ratings assigned in the SV-6 to information exchanges going across a particular link or being processed by a particular subsystem in the SV-1. In this way, although criticality ratings are assigned at the subsystem/link level, it is still the underlying information residing in the SV-6 that ultimately determines criticality to the mission.

It is important to note that these ratings would be different from the "key interface" designations that can already be assigned to links on the SV-1. The current "key interface" designation can stand for a variety of things to include the following (DoDa, 2007:5-2):

- The interface spans organizational boundaries
- The interface is mission critical
- The interface is difficult or complex to manage
- There are capability, interoperability, or efficiency issues associated with the interface

The problem that exists is although a link may be designated a "key interface" because it is mission critical, it is impossible to discern due to the fact that there are multiple other reasons why it could also be designated a "key interface." A person looking at the SV-1 has no indication regarding the rationale for why it was designated a "key interface." Further, currently only interfaces can be designated "key" in the SV-1, whereas the subsystems in the SV-1 also need to be considered for "key" designation since they are responsible for processing and generating the information going across the interfaces.

Ultimately, the benefit provided by assigning criticality ratings to the links and subsystems in the SV-1 is a reduction in the amount of data a person would have to consider in developing Level 2 cyber SA, whether it is the individual weapon system operator desiring Level 2 cyber SA on his or her own system, or the individual responsible for developing Level 2 cyber SA across multiple weapon systems under the span of control of a particular commander. Instead of considering the importance of hundreds or thousands of individual pieces of information per weapon system to the operational mission, one would only have to understand the importance of a small number of subsystems/links per weapon system. Although assessing impact of cyber status across multiple platforms upon the operational mission will still be a significant challenge, it at least places achievement of Level 2 cyber SA for the commander in the realm of possibility.

The actual changes to the SV-1 could be fairly simple. In Figure 9, assuming the weapon platform being analyzed is "Node A", rolled up mission criticality ratings could be assigned to each of the interfaces touching Node A and to each of the subsystems contained within the platform that connect to those interfaces. As acquisition systems document the criticality of their systems and network links, based upon the underlying information being processed or transmitted, cyber SA correlation centers would have a source for gathering data to better understand mission impacts resulting from a weapon system's cyber status. Understandably, an accurate assessment in real time of multiple weapon system's cyber status and their impact upon joint operations is an extremely difficult task. Those responsible for the task will require the development of automated tools for correlating cyber status with the operational mission, along with SA displays

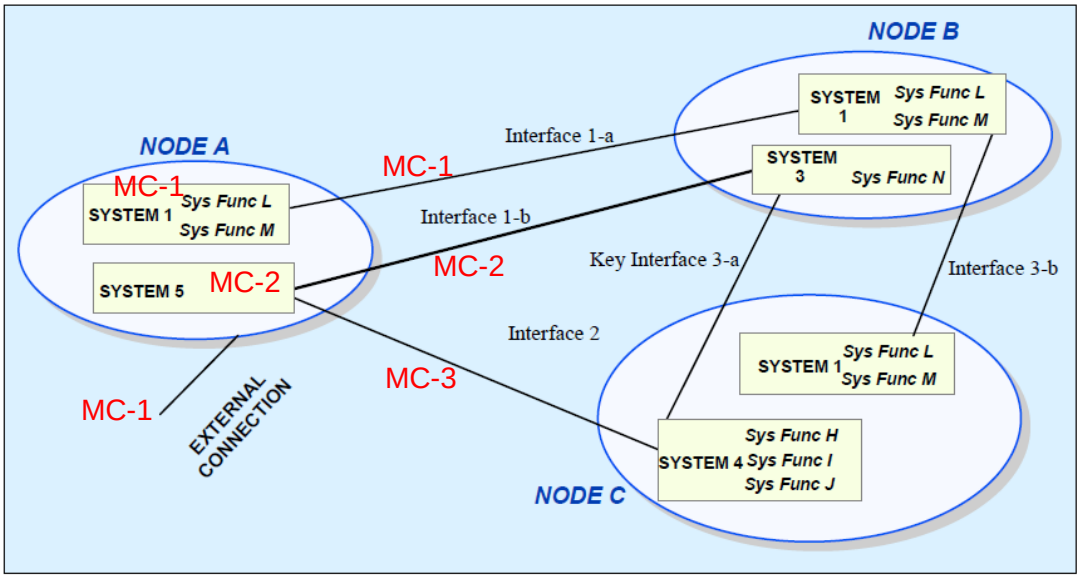

Figure 9 – Modified SV-1: Mission Criticality

that provide information in an easy to understand manner. These tools for providing Level 2 cyber SA have yet to be developed. However, by adequately developing the DoDAF architecture products discussed above, acquisition systems can play an integral part in generating the underlying information and data on which automated tools and SA displays would depend.

It is also important to note that mission criticality ratings are important not only for commanders whose span of control involves a large number of systems, but also for the individual weapon systems themselves. Weapon systems, whether an air platform, a ship, or a command and control system, often depend upon certain information coming from outside sources in order to successfully prosecute their mission. As such, they also need to have an understanding of the cyber status of the systems upon which they are dependent for performing their mission. Methodologies and procedures for reporting

information incidents and cyber status downgrades to other systems downstream from the infected information source need to be developed (Grimalia and Fortson, 2007:210-211). This "mission mapping" is a difficult and complex process that will require much time and effort, along with automated tools. Once again, the DoDAF cyber SA architecting discussed earlier can at least provide a starting point for gathering the underlying information needed.

The importance of a weapon system knowing the cyber status of other weapon systems upon which its mission is dependent becomes more serious when one realizes that it is not always simply a question of whether or not a particular system or network is up or down. In some cases, an adversary could be in the system changing data without affecting the performance of the system or the network. In such cases, an end node may not notice any difference in the services being provided, and as a result, is likely to trust what is coming over the network. To combat this tendency, notification of potential infections which may be reducing the integrity of the data need to be passed to weapon systems downstream who are using the data. Depending upon the importance of the assigned mission, the increased risk from potentially altered data, and the availability of other sensors/sources to verify information on the network, the weapon system operator may choose to continue or cancel a particular mission.

Achieving Level 3 Cyber SA – Cognitive Processes

Derived requirements for all acquisition in developing Level 3 cyber SA for the commander do not exist. This is primarily because projection of the future state of friendly system cyber status and its impact upon the operational mission is a product of the cognitive activity of the commander/decision maker. Based upon past experiences

and situations, in combination with various level of education and training, different commanders and their support staffs will differ in their capability at, for example, predicting the amount of time it will take to recover from a downed link or the time it will take for our forces to respond to a cyber incident and take out the adversary creating the problems. As for predicting an adversary's next move in the cyber domain, other cyber SA elements, such as developing an understanding of an adversary's intent and their capabilities are required to give a commander Level 3 cyber SA. What is important to note, however, is these cyber SA elements do not drive requirements for all acquisition. They may drive requirements for specific intelligence and operational capabilities that lead to doctrinal changes or new material solutions, but they do not drive requirements for all acquisition. As examples, to help provide Level 3 cyber SA, automated prediction tools for better understanding the future cyber situation, or network mapping tools to better understand the adversary's network topology could potentially be developed . However, the development of these tools would result in their own acquisition programs, not a derived requirement for all acquisition.

Additional Cyber SA Concerns

Maintenance of Cyber SA Architecture

Maintaining a weapon system's cyber SA architecture is not a one-time process that exists only during the design and development portion of the acquisition cycle. As a weapon system's mission evolves throughout its lifecycle, mission criticality ratings of particular nodal links and systems on a weapon platform will likely change. As a result, the system's cyber SA architecture will also need updated. In addition, the quick technology change cycles within networking and software will likely drive the need to

alter SA tools, interfaces, etc. within the weapon system's cyber SA architecture. If SA architecture processes end upon the weapon system going into production, cyber SA correlation efforts will soon fail due to outdated information and inaccurate mission criticality ratings. As such, acquisition programs need to ensure there is a reliable process of transferring the responsibility of cyber SA architecture maintenance to the operational user.

Doctrinal Concerns

As discussed previously, cyberspace can be looked at from two different perspectives, either as a supporting infrastructure for other domains or as its own operational warfighting domain. Within the higher level DoD documents we examined in Chapter 2, language that addressed the need for situational awareness supported both perspectives of cyberspace. However, within AF service-level doctrine addressing cyberspace, language appears to be trending toward an emphasis on situational awareness activities that primarily see cyberspace as its own warfighting domain.

AF Doctrine Document 2-5, Information Operations, without ever using the specific language of cyber SA, defines some characteristics of cyber SA that would fit under its umbrella. Lumped under "Network Warfare Support (NS)", AFDD 2-5 states "NS is critical to Net Attack and Net Defense actions to find, fix, track, and assess both adversaries and friendly sources of access and vulnerability for the purpose of immediate defense, threat prediction and recognition, targeting, access and technique development, planning, and execution in NW Ops (Department of the Air Force [DAF], 2005:21)." It goes on to state:

> Products resulting from this collection and exploitation process include the network order of battle and parametric data reflecting the characteristics of

> various network threat and target systems. NS data are used to produce intelligence, or provide targeting and engagement data for electronic, network, or influence attack. Specifically, NS provides profiling, event analysis, open source review, as well as pattern analysis in support of Net Defense and countermeasure development. Likewise, NS provides nodal and system analysis and engineering to identify potential vulnerabilities in adversary systems to support Net Attack. (DAF, 2005:21)

Most of the activities mentioned are activities associated with the development of information and situational awareness that supports net warfare (i.e. net attack and net defense). Very little to no language is spent on encouraging the development of cyber situational awareness products that assist with determining how changes in the network may be affecting other operational domains. In other words, situational awareness in support of cyberspace as its own warfighting domain is emphasized over situational awareness in support of cyberspace as a key supporting infrastructure.

AF Doctrine Document 2-11, Cyberspace Operations, indicates the need for continuous intelligence preparation of the operational environment (IPOE) due to the "vastness, complexity, volatility, and rapid evolution of cyberspace (DAF, 2008: 9)." The document also mentions the need for IPOE and SA in cyberspace for effective defensive and offensive operations. It appears, however, that the focus tends to be on offensive operations and its tie-in to the targeting cycle. In general, the definition of SA within the cyber domain is focused on understanding the adversary's networks and its weaknesses, the likely effects on the adversary's networks resulting from attacks upon those weaknesses, and the impacts to the adversary's other domains and infrastructure that rely upon the cyber domain. The resulting cyber SA that is generated is then integrated into the Joint Forces Commander's planning and execution process for attacking the adversary, potentially with cyber attack capabilities. Once again, the focus is on how we

can develop situational awareness to support the use of the network as its own operational domain (i.e. attacking the enemy's network).

This becomes more clear when examining Figure 10.

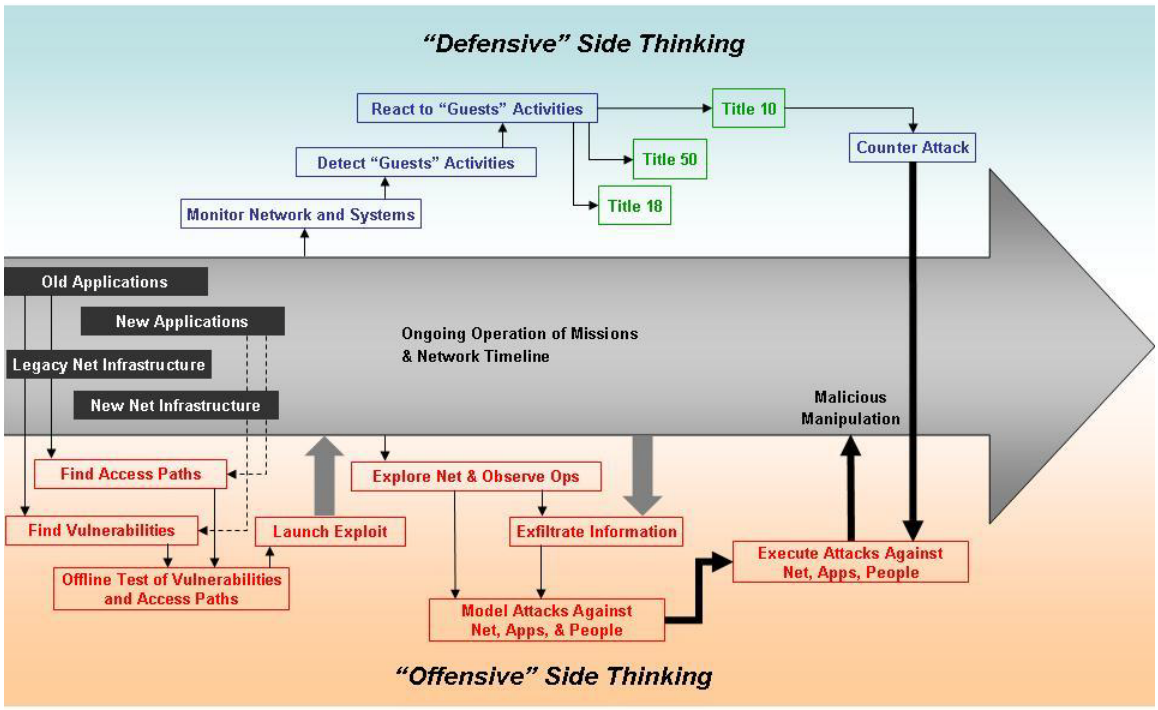

Figure 10 – Anatomy of a Cyberspace Operation (DAF, 2008:35)

On the offensive network attack side, situational awareness activities such as "find access paths", "find adversary network vulnerabilities", and "explore adversary net and observe operations" are listed. On the defensive side, the situational awareness activity of "monitor our own networks and systems" is listed. What is interesting to note is that on both sides they culminate in some type of cyber attack. The emphasis is on the use of cyberspace as its own operational warfighting domain. There is no mention of cyberspace operations as a supporting infrastructure to the other warfighting domains. Maybe it is implicitly implied in the "defensive" side thinking, but it is not clear. Ideally, as shown in Figure 11, an additional step between "detect guest activities" and "react to

guest's activities" named "determine and prioritize impact to commander's mission" should be included. Also, the step "react to guests activities" should be changed to "react to guests activities based upon impact to commander's overall mission."

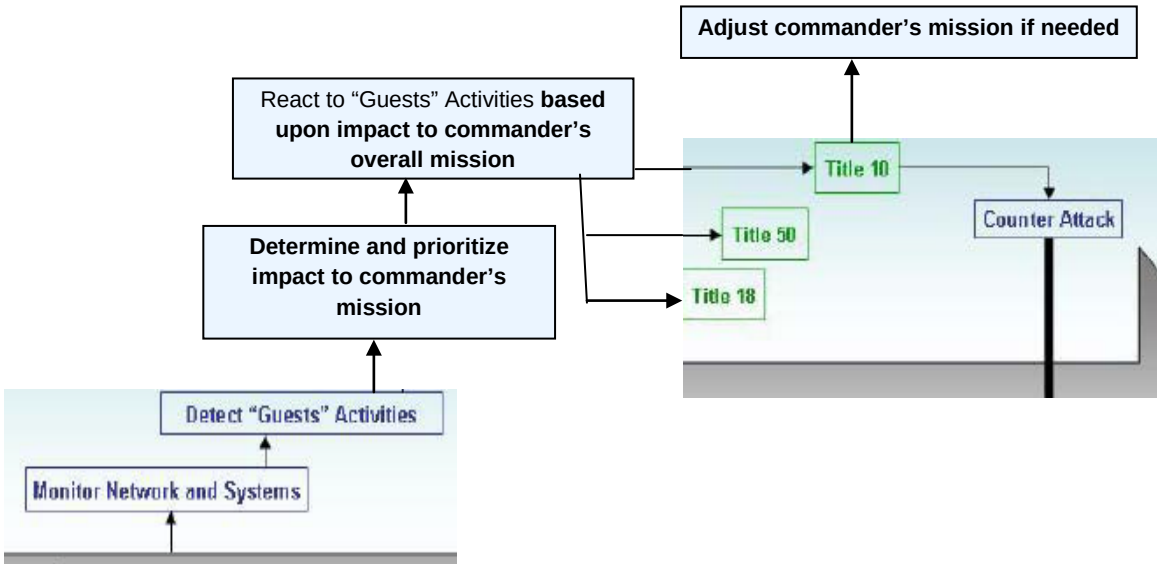

Figure 11 – Anatomy of Cyberspace Operation – "Defensive" Modification

This early research raises the concern that as cyberspace is seen more and more as a way to create effects similar to other domains (i.e. air, space, land, sea), even less emphasis may be put on cyberspace's supporting role to those domains. If this were to occur, the likelihood of achieving Level 2 cyber SA will lessen as cyber SA investment is primarily directed towards activities that support offensive net warfare activities.

IV. Conclusions and Recommendations

The provision of cyber SA for the commander is an extremely difficult task. When one observes the minimal amount of work accomplished to date in this area and the grand scope of activities that need to occur, even the idea of developing a comprehensive cyber SA picture for the commander can quickly become overwhelming. With DoD continuing to advocate a net-centric vision, pushed by the pace of information technology developments and resulting in ever increasing connectedness of our forces, the already difficult problem of trying to understand cyber status and cyber dependencies will see exponential growth. The bottomline is the establishment of cyber SA for the commander will only continue to get more difficult with time. In addition, the growth in connectedness provides ever increasing opportunities for the adversary to gain access to our networks in an attempt to create havoc with our military operations.

As such, the DoD cannot fail in beginning to address problems related to cyber SA and identifying solutions. The development of solutions will require significant effort from both the operational and acquisition communities. Neither can do it alone and success will only result from the synergy created from efforts in both camps. The acquisition world cannot implement the right solutions if the operational world does not provide a proper framework or context in which the solutions are expected to work. On the other hand, the operational world will never be able to achieve cyber SA for the commander if the acquisition world does not begin, in conjunction with warfighters, to fully integrate cyber SA thinking into their weapon system design and development. Based upon the synergy that is needed between the operational and acquisition communities, the following recommendations and areas for future research are provided:

Recommendations:

The following list of recommendations is provided:

- STRATCOM lead an effort to develop a SA enterprise architecture
- Pursue stairstep implementation of cyber SA architecture
    - Near-term integration of cyber SA tools at platform level
    - Level II cyber SA experimentation at mission area level
    - Implementation at combatant commander level
- Consider incorporation of cyber SA language into NR-KPP
- Ensure inclusion of cyber threats in STARs
- Develop modeling tools to assess cyber threats
- Ensure cyber doctrine keeps well-rounded perspective (i.e. cyberspace as its own domain and cyberspace as supporting infrastructure to other domains)

STRATCOM Lead an Effort to Develop a SA Enterprise Architecture

SRATCOM needs to lead an effort to develop a cyber SA enterprise architecture as a framework for acquisition programs to follow in implementing cyber SA within system design and development. Initially, the cyber SA architecture should focus on providing Level I cyber SA implementation guidance, to include definition of cyber SA data elements, formats, and transmission protocols. These cyber SA enterprise architecture products will ensure consistency of implementation across acquisition programs, facilitating consolidation and correlation of cyber SA data in the future. As organizational structures and responsibilities for cyber SA are better refined by the operational/cyber community, the SA enterprise architecture should include a concept of

operations for providing cyber SA Level II to the operational commander, to include identification of organizations and locations responsible for receiving and correlating cyber SA data. A cyber SA CONOPs will allow acquisition programs to implement the appropriate interfaces and communication methods to ensure cyber SA data is properly transmitted to the designated location.

Pursue Stairstep Implementation of Cyber SA Architecture

It is recognized that the previous recommendation of developing a cyber SA enterprise architecture will likely be extremely difficult and at times, a cumbersome process. This is due not only to the diverse and large system of systems environment in which cyber SA is expected to operate, but also due to the fact that the DoD continues to wrestle with establishing command authorities and an organizational structure to conduct the cyberspace mission. Due to the difficulties of attempting to establish a cyber SA architecture across the whole DoD enterprise, it is recommended that the DoD take a stairstep approach. This stairstep approach (Figure 12) should start at the weapon platform level, where the acquisition community can provide significant assistance, before moving to mission area and combatant commander levels.

Near-Term Integration of Cyber SA Tools at Platform Level

Although a cyber SA enterprise architecture does not currently exist, weapon system platforms should begin implementing cyber SA tools within their own platform architectures to provide cyber SA to the platform operator. Implementation of tools should be pursued not only by software intensive C4I systems, which in many instances, already use cyber SA tools such as IDS's, but also aircraft, vehicles, ships, etc. that have

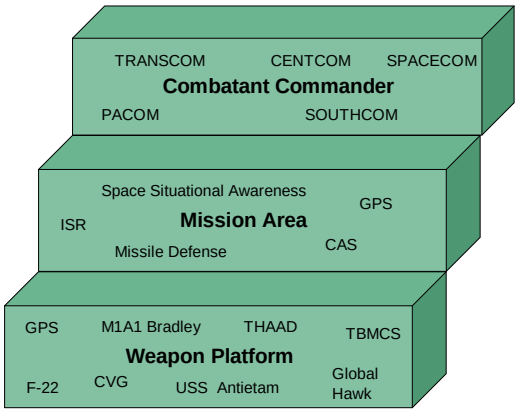

Figure 12 – Cyber SA Architecture Stairstep Implementation

on-board cyber components attached to tactical networks or the GIG through satellite communications, wireless transmissions, etc. Efforts at integrating cyber SA into platform architectures will not only hopefully prepare the weapon systems for quicker and easier integration into a future cyber SA enterprise architecture, but also provide a means for localized experimentation in the collection and correlation of cyber SA data. Lessons learned from such use can provide valuable insight for the STRATCOM led effort to develop a functioning cyber SA architecture.

Level 2 Cyber SA Experimentation at Mission Area Level

The research, acquisition, and operational communities should initiate smaller scale experimental efforts to develop, examine, and refine tools for consolidating cyber status and mission criticality data across a particular mission area. For example, a Predator ISR mission could be simulated using a subset of the networks and nodes shown in Figure 13. Various cyber SA data collection, dissemination, and correlation methods

could be tested within the limited ISR mission framework. Through such efforts, Level 1 cyber SA information could be matured as part of the process of developing the cyber SA enterprise architecture. In addition, ideas for Level II cyber SA correlation software tools and cyber SA displays that may sit at a cyber correlation center could be examined and refined in preparation for implementing the cyber SA architecture at a combatant commander level, where the number of systems involved would be considerably larger. Numerous, lower cost experiments which encourage innovative ideas and allow room for failure are essential if large scale cyber SA solutions across a combatant commander's area of responsibility are ever to succeed.

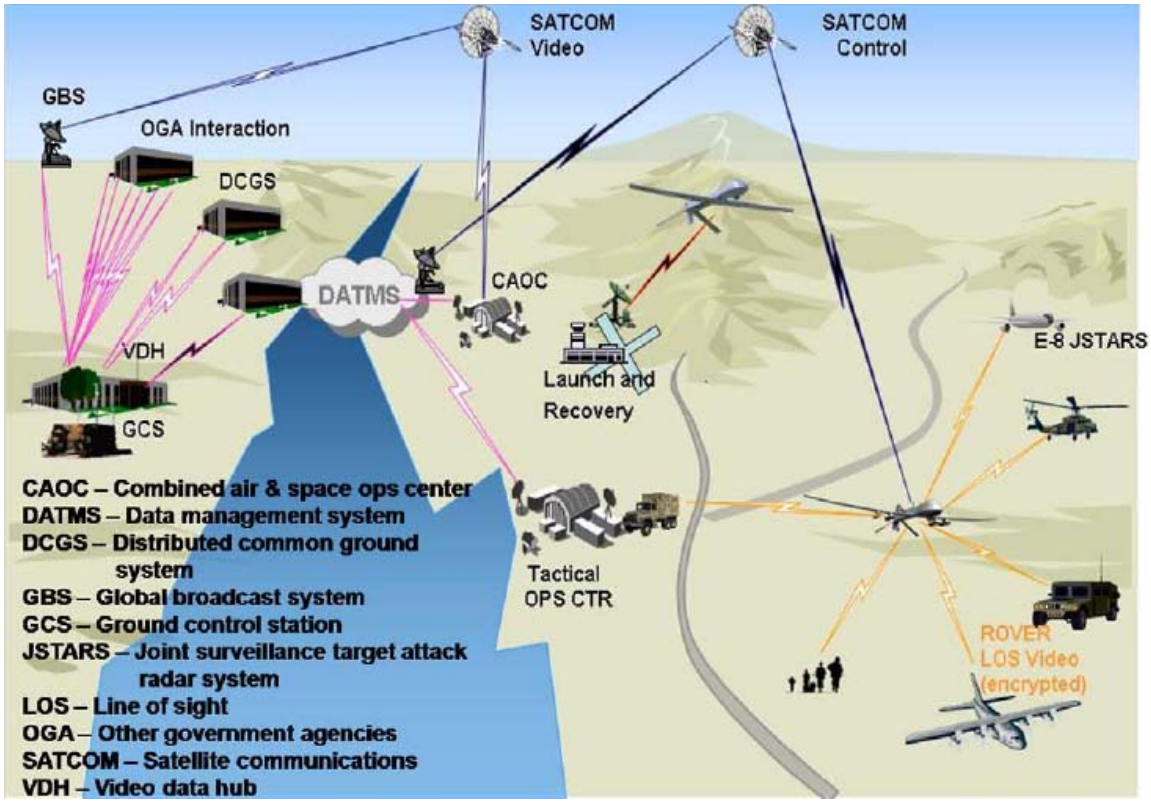

Figure 13 – Predator Network and Nodes (DAF, 2008:5)

Implementation at Combatant Commander Level

As cyber SA methodologies and tools prove themselves out in smaller scale experiments at the mission-level, they can begin to be integrated into cyber correlation centers at larger scale exercises where they can be refined further before deployment in support of providing cyber SA across a combatant commander's area of responsibility.

Consider Incorporation of Cyber SA Language into NR-KPP

To better drive acquisition programs towards considering cyber SA during system design and development, ASD(NII)/DoD CIO should consider including implementation of cyber SA strategies and compliance with cyber SA enterprise architectures as a sixth element to the NR-KPP. As part of this addition, the NR-KPP threshold and objective compliance statements (Table 4) would also need to include the cyber SA requirement language.

Further, a requirement for programs to complete the modified SV-1, discussed in Chapter 3, showing mission criticalities (see following recommendation) of nodal systems and links needs to be added to the NR-KPP requirements. Currently, the SV-1 is one of only several views that are not required to be completed by acquisition programs in fulfillment of NR-KPP requirements (Table 5). The addition of the modified SV-1 would assist the acquisition program in understanding its nodal and link mission dependencies better for correlation with cyber status and achievement of Level 2 cyber SA for the weapon system. In addition, the modified SV-1 would provide a source of information to pull from as tools and methodologies are developed for establishing Level 2 cyber SA at the mission and combatant commander levels.

Last, cyber SA language needs to be added to the Interoperability and Supportability Assessor's Checklist (CJCS, 2006:D-C-1 to D-C-14 – See Appendix A) used by the Joint Staff J-6 to certify the NR-KPP in acquisition documents and Information Support Plans (ISPs). This is needed to make it clear to program offices that cyber SA is seen as an as important piece of the NR-KPP. As a start, a basic question

Table 4 – NR-KPP Compliance Statement (CJCS, 2008:E-21)

KPP	Threshold (T)	Objective (O)
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD Information Enterprise Architecture (DOD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, and/or service must fully support execution of all operational activities and information exchanges identified in DOD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include 1 Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD IEA, excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GESPs, necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an ATO by the DAA, and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.

within the “Detailed Architecture Analysis” section of the checklist could be added, such as “Do the document architecture views reflect information exchanges required for establishing weapon system cyber SA?” Once a larger cyber SA enterprise architecture is fleshed out, a question such as, “Are cyber SA data elements and information exchanges compliant with the DoD’s cyber SA enterprise architecture?” could be added along with more detailed questions as needed.

Table 5 – NR-KPP Products Matrix (CJCSI, 2000:E-19)

Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)																Data/Service Exposure Sheets	IA Compliance	GTG Compliance
		AV-1 /AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X
X	Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)																			
Note 1	Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services.																			
Note 2	The TV-1 and TV-2 are built using the DISRonline and must be posted for compliance.																			
Note 3	The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance																			
Note 4	Only required for Milestone C, if applicable (see Note 1)																			
Note 5	The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change.																			

Ensure Inclusion of Cyber Threats in System Threat Assessment Reports (STARs)

Acquisition programs need to coordinate with the intelligence community and ensure cyber threats to their weapon system are included in the STAR required for each

milestone during system design and development. Through inclusion of cyber threats, acquisition programs can achieve a portion of Level 3 Cyber Projection SA by adapting their cyber SA tools to better detect future cyber threats.

Develop Modeling Tools to Assess Cyber Threats

In an effort to adapt cyber SA tools to future cyber threats, acquisition programs will require modeling tools in which they can test their weapon systems against future adversary cyber threats. Within the air domain, numerous physics based modeling tools exist to evaluate how a new aircraft design will fair against current and future adversary aircraft and surface-to-air missiles. Based upon the results, the design team can then modify the design in order to better fight through the adversary systems and survive. In a similar manner, modeling tools to examine current and future cyber threats against a weapon system's cyber architecture will allow program offices to adapt their weapon systems and stay a step ahead of the adversary. Such tools will assist programs in preparing their weapon systems to fight through cyber attacks and survive.

Ensure Cyber Doctrine Keeps Well-Rounded Perspective

As discussed in Chapter 3, as cyberspace doctrine develops over the next several years, the DoD needs to ensure that the role of cyberspace in supporting other warfighting domains does not lose out to the glitzier concepts of network attack and computer network exploitation. Otherwise, funding to support initiatives to provide Level II cyber SA for the commander will fail to materialize.

Areas for Future Research

Several areas of future research to better understand the development of a cyber SA architecture and the maturation of cyber SA for the operational commander are provided.

Development of a Cyber SA MIB

Additional research to identify a common cyber SA MIB that establishes a weapon system's cyber status is needed. The research could help identify a single cyber SA MIB for all weapon systems, or more likely identify several cyber SA MIBs for major categories of weapon systems (i.e. C4I/software intensive systems, tactical weapon platforms, satellites, etc.) The research needs to reduce the large number of parameters and measurements that exist today in monitoring network/system software status into a reasonable number that meets the needs of a DoD cyber SA enterprise architecture. A common SA MIB is essential for ensuring acquisition systems are implementing common cyber SA solutions in their architectures that will allow transmission, consolidation and correlation of the data as needed to support cyber SA beyond the weapon platform level.

Modeling for Cyber SA Correlation Level

One of the most difficult tasks in creating cyber SA for the commander at higher levels, such as a warfighting combatant commander is the difficulty of implementing a cyber SA architecture within a large system of systems environment. If a cyber SA MIB is established and cyber SA is developed at the platform level, modeling to determine the feasibility of extending cyber SA to the mission and higher levels should be accomplished in support of developing an enterprise cyber SA architecture. A likely result could be that disseminating, consolidating, and correlating cyber SA data at larger

command levels is not technically or organizationally feasible. Modeling will help cyber SA architects define at what level of command a consolidated cyber SA picture is feasible and operationally usable in the decision-making process.

Investigate Space SA Architecture for Application to Cyber SA Architecture

In developing a cyber SA architecture, an in-depth look at what the space community is implementing for their space SA architecture may provide valuable. STRATCOM has designated the Joint Space Operations Center (JSpOC) at Vandenburg AFB, CA, under the Joint Functional Component Command for Space (JFCC-SPACE) as the lead for gaining and maintaining space SA. Similar to cyber SA, gaining and maintaining space SA requires the gathering and analysis of information from a large number of diverse systems across multiple organizations. As STRATCOM is the lead combatant command for both space and cyber operations, tools and methodologies, organizational constructs, space acquisition practices, and architecture products JFCC-SPACE is encouraging and/or using for improved space SA could be examined for applicability to the cyber SA architecture.

Bibliography

Arnborg, S. and others. "Information Awareness in Command and Control: Precision, Quality, Utility," *Proceedings of the Third International Conference on Information Fusion*, 25-32, 2000.

Assistant Secretary of Defense (Networks & Information Integration)/DoD Chief Information Officer (ASD[NII]/CIO). *Information Assurance*. DoDD 8500-01E. Washington: ASD[NII]/CIO, 23 April 2007. http://www.defenselink. mil/cio-nii/policy/instructions.shtml.

Bruey, Douglas. "SNMP: Simple? Network Management Protocol." RaneNote 161 (December 2005). http://www.rane.com/note161.html. 1 June 2009.

Case, J. and others. "A Simple Network Management Protocol." RFC1157, Internet Engineering Task Force (1990). http://www.ietf.org/rfc/rfc1157.txt?number=1157. 1 June 2009.

Clement, Michael R. *A Holistic Management Architecture for Large-Scale Adaptive Networks*. MS Thesis, Naval Postgraduate School, Monterey, CA, September 2007

Defense Acquisition University (DAU) Continuous Learning Course, CLM 029, Net-Ready Key Performance Parameter (NR-KPP). DAU, Fort Belvoir, VA, March 2009.

Department of the Air Force (DAF). *Information Operations.* Air Force Doctrine Document (AFDD) 2-5, 11 January 2005. https://www.doctrine.af.mil.

-----. "*Cyberspace Operations*. AFDD 2-11, 24 October 2008. https://www.doctrine. af.mil

Department of Defense (DoD)a, *DoD Architecture Framework (DoDAF) Volume II: Product Descriptions*, Version 1.5, 23 April 2007.

DoDb, *Technical Specifications for the Core Architecture Data Model (CADM)*, Version 1.5, 23 April 2007.

DPS Telecom, "SNMP Tutorials". Excerpt from website training tutorials. n.pag. http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php. 1 June 2009.

Endsley, Mica R. "Design and Evaluation for Situation Awareness Enhancement," *Proceedings of the Human Factors Society 32nd Annual Meeting*. 97-101. Santa Monica, CA: Human Factors Society, 1988.

-----. "Theoretical Underpinnings of Situation Awareness: A Critical Review" in *Situation Awareness Analysis and Measurement.* Eds. M.R. Endsley and D.J. Garland. Mahwah, NJ: Lawrence Erlbaum Associates.

-----. "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, 37(1): 32-64 (March 1995).

Endsley, Mica R. and others, "Situation Awareness Information Requirements for Commercial Airline Pilots**,"** ICAT-98-1. Cambridge, MA: Massachusetts Institute of Technology International Center for Air Transportation, September 1998.

Grimalia, Michael R. and Larry W. Fortson. "Towards an Information Asset-Based Defensive Cyber Damage Assessment Process," *Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications*. 206-212, 2007.

Grimalia, Michael R. and others. "*An Automated Information Asset Tracking Methodology to Enable Timely Cyber Mission Impact Assessment,*" Air Force Institute of Technology (AU), Wright Patterson AFB OH, 2008 (ADA486813).

Hughes, Evan and Anil Somayaji. "Towards Network Awareness," *Proceedingsof the 19th Large Installation System Administration Conference.* 113-124, 2005.

Joint Requirements Oversight Council (JROC). *Functional Concept for Battlespace Awareness Version 2.1*. 31 December 2003 http://www.dtic.mil/futurejointwarfare/jfc.htm.

Joint Staff. *DoD Dictionary of Military and Associated Systems.* JP 1-02. Washington: GPO, 17 March 2009.

-----. *Interoperability and Supportability of Information Technology and National Security Systems*. CJCSI 6212.01E. Washington: Joint Staff J-6, 15 December 2008. http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm

-----. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. JP 2-01.3. Suffolk, VA: US Joint Forces Command, 24 May 2000.

"JTF-GNO Mission." Excerpt from JTF-GNO website. n.pag. https://www.jtfgno.mil/misc/mission.htm. 19 May 2009.

Salerno, John J. and others. "A Situation Awareness Model Applied to Multiple Domains," in *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2005,* edited by Belur V. Dasarathy, Proceedings of SPIE Vol. 5813 (SPIE, Bellingham, WA, 2005), 65-74.

Shaw, Alfred K. *A Model for Performing Mission Impact Analysis of Network Outages*. MS thesis, AFIT/GCS/ENG/07-10. Graduate School of Engineering and Managemetn, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2007

"Situational Awareness Reports." Excerpt from JTF-GNO website. n.pag. https: //www.jtfgno.mil/ operations/sar/2009/index.html. 19 May 2009.

Tadda, George and others. "Realizing Situation Awareness in a Cyber Environment," in *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2006*, edited by Belur V. Dasarathy, Proceddings of SPIE Vol. 6242 (SPIE, Bellingham, WA, 2006), 624204-1 – 624204-8.

United States Strategic Command. *Deterrence Operations Joint Operating Concept Version 2.0.* December 2006 http://www.dtic.mil/futurejointwarfare/joc.htm.

Williams Technology Consulting Services. "What is SNMP?" Excerpt from SNMP for the Public Community website. n.pag. http://www.wtcs.org/snmp4tpc/snmp.htm. 1 June 2009.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
18-06-2009	Graduate Research Paper	Sep 2008 – Jun 2009

4. TITLE AND SUBTITLE
Integration of Cyber Situational Awareness (SA) into System Design and Development

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Chase, Lee E., Maj, USAF

5d. PROJECT NUMBER
ENS 09-153

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ISE/ENV/09-J02

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Maj William F. Dobbs
HQ USAF/CVAQ
1670 Air Force Pentagon
Washington DC 20330
Commercial: 703-588-8586

10. SPONSOR/MONITOR'S ACRONYM(S)
AF/CVAQ

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States

14. ABSTRACT
Cyber situational awareness (SA) is the correlation of network status to operational impact. This capability is increasingly important for commanders and individual weapon system platforms as the DoD continues its exploitation of net-centric operations. To achieve higher maturity levels of cyber SA, the acquisition community needs to act as an enabler by making cyber issues an integral part of early system design and development. This paper identifies key cyber characteristics needing consideration and recommends improvement to acquisition policy and guidance, including the net-readiness key performance parameter (NR-KPP) and the DoD Architecture Framework (DoDAF).

15. SUBJECT TERMS
Cyber situational awareness, net-readiness key performance parameter, architecture, cyber status

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. John Colombi, AFIT/ENV
U	U	U	UU	91	19b. TELEPHONE NUMBER *(Include area code)* 937-255-3636 x3347

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18

Form Approved
OMB No. 074-0188